REQUEST FOR QUOTE (RFQ)

GSC-QF0B-14-32845

Security Engineering and Operations Support

in support of:

GSA IT, Office of the Chief Information Security Officer

Issued to:
ALL HUBZONE CONTRACTORS UNDER GSA Schedule IT 70
Special Item Number 132-51

The Contractor's Basic GSA Schedule contract is applicable to the Task Order that is awarded under this RFQ

Conducted under FAR 8.4. Do not intend to use FAR 15 principles.

Issued by:
General Services Administration
Federal Systems Integration and Management Center (FEDSIM)
1800 F Street NW
Suite 3100 (QF0B)
Washington, DC 20405

May 28, 2014
FEDSIM Project Number GS00658

1.1 ORDER TYPE

The contractor shall perform the effort required by this Task Order (TO) on a hybrid Firm-Fixed-Price (FFP) and Time-and-Materials (T&M) basis. The work shall be performed in accordance with all Sections of this TO and the offeror's General Services Administration (GSA) Multiple Award Schedule (MAS), under which the resulting TO will be placed. An acronym listing to support this Request for Quote (RFQ) is included in Section 9 - List of Attachments, Attachment H.

1.2 SERVICES AND PRICES

Long-distance travel is defined as travel over 50 miles. Local travel will not be reimbursed.

The following abbreviations are used in this price schedule:

CLIN	Contract Line Item Number
FFP	Firm-Fixed-Price
NTE	Not-to-Exceed
ODC	Other Direct Cost
T&M	Time-and-Materials

1.2.1 BASE PERIOD:

FFP LABOR CLIN

CLIN	Description	QTY	Unit	Total Firm Fixed Price
0001	Task 1	12	(month)	$

T&M LABOR CLINS

CLIN	Description	Total Hours	Total NTE Ceiling
0002	Labor (Tasks 2-10)	Insert total hours for all labor identified below	

Labor Category	Hours	Hourly Rate
List specific labor categories from your IT Schedule 70 contract.		
TOTAL HOURS		

COST REIMBURSEMENT TRAVEL and ODC CLINs

CLIN	Description		Total Ceiling Price
0003	Long Distance Travel Handling Rate ___% (fill in)	NTE	$ 15,000.00
0004	ODCs Handling Rate ___% (fill in)	NTE	$ 3,000.00

TOTAL BASE PERIOD CLINs: **$_____**

1.2.2 FIRST OPTION PERIOD:

FFP LABOR CLIN

CLIN	Description	QTY	Unit	Total Firm Fixed Price
1001	Task 1	12	(month)	$

T&M LABOR CLINS

CLIN	Description	Total Hours	Total NTE Ceiling
1002	Labor (Tasks 2-10)	Insert total hours for all labor identified below	

Labor Category	Hours	Hourly Rate
List specific labor categories from your IT Schedule 70 contract.		
TOTAL HOURS		

COST REIMBURSEMENT TRAVEL and ODC CLINs

CLIN	Description		Total Ceiling Price
1003	Long Distance Travel Handling Rate ___% (fill in)	NTE	$15,000.00
1004	ODCs Handling Rate ___% (fill in)	NTE	$0.00

TOTAL FIRST OPTION PERIOD CLINs: **$_____**

GRAND TOTAL ALL CLINs: **$_____**

1.2.3 SECOND OPTION PERIOD

FFP LABOR CLIN

CLIN	Description	QTY	Unit	Total Firm Fixed Price
2001	Task 1	12	(month)	$

T&M LABOR CLINS

CLIN	Description	Total Hours	Total NTE Ceiling
2002	Labor (Tasks 2-10)	Insert total hours for all labor identified below	

Labor Category	Hours	Hourly Rate
List specific labor categories from your IT Schedule 70 contract.		
TOTAL HOURS		

COST REIMBURSEMENT TRAVEL and ODC CLINs

CLIN	Description		Total Ceiling Price
2003	Long Distance Travel Handling Rate ___% (fill in)	NTE	$ 15,000.00
2004	ODCs Handling Rate ___% (fill in)	NTE	$ 0.00

TOTAL SECOND OPTION PERIOD CLINs: $_____

GRAND TOTAL ALL CLINs: $_____

1.2.4 THIRD OPTION PERIOD

FFP LABOR CLIN

CLIN	Description	QTY	Unit	Total Firm Fixed Price
3001	Task 1	12	month	$

T&M LABOR CLINS

CLIN	Description	Total Hours	Total NTE Ceiling
3002	Labor (Tasks 2-10)	Insert total hours for all labor identified below	

Labor Category	Hours	Hourly Rate
List specific labor categories from your IT Schedule 70 contract.		
TOTAL HOURS		

COST REIMBURSEMENT TRAVEL and ODC CLINs

CLIN	Description		Total Ceiling Price
3003	Long Distance Travel Handling Rate ___% (fill in)	NTE	$15,000.00
3004	ODCs Handling Rate ___% (fill in)	NTE	$ 0.00

TOTAL THIRD OPTION PERIOD CLINs: $_____

GRAND TOTAL ALL CLINs: $_____

1.2.5 FOURTH OPTION PERIOD

FFP LABOR CLIN

CLIN	Description	QTY	Unit	Total Firm Fixed Price
4001	Task 1	12	month	$

T&M LABOR CLINS

CLIN	Description	Total Hours	Total NTE Ceiling
4002	Labor (Tasks 2-10)	Insert total hours for all labor identified below	

Labor Category	Hours	Hourly Rate
List specific labor categories from your IT Schedule 70 contract.		
TOTAL HOURS		

COST REIMBURSEMENT TRAVEL and ODC CLINs

CLIN	Description		Total Ceiling Price
4003	Long Distance Travel Handling Rate ___% (fill in)	NTE	$15,000.00
4004	ODCs Handling Rate ___% (fill in)	NTE	$ 0.00

TOTAL FOURTH OPTION PERIOD CLINs: $_____

GRAND TOTAL ALL CLINs: $_____

1.3 SECTION 1 - SUPPLIES OR SERVICES AND PRICE/COSTS TABLES

1.3.1 INDIRECT/MATERIAL HANDLING RATE

Travel and ODC costs incurred may be burdened with the contractor's indirect/material handling rate in accordance with the contractor's Schedule Contract. If no indirect/material handling rate is allowable in accordance with the contractor's Schedule Contract, no indirect/material handling rate shall be applied to or reimbursed on such costs.

1.3.2 LIMITATION ON OTHER DIRECT COSTS

ODC costs incurred on GSA Schedule TOs are limited to a maximum of $3,000 over the life of the TO.

1.4.1 TIME & MATERIAL LABOR MIX AND LEVEL OF EFFORT

The labor mix and level of effort specified in the contractor's quote and incorporated into this order are for estimation purposes. The contractor may re-allocate, with prior written approval of the Federal Systems Integration and Management Center (FEDSIM) Contracting Officer's Representative (COR), the number of hours by labor category, within each labor CLIN as needed to effectively manage the project, provided the total funded labor cost and total hours are not exceeded. Any additional labor categories or increases to total hours or increases to ceilings required during performance must be approved by the Contracting Officer (CO) and added to the TO by modification.

2.1 BACKGROUND

Federal Acquisition Service (FAS) serves as the acquisition and procurement arm of the Federal Government, offering equipment, supplies, telecommunications, and integrated information technology (IT) solutions to Federal agencies. The Public Building Service (PBS) is charged to provide superior workplaces for federal customer agencies at good economies to the American taxpayer. The GSA has recently consolidated Service/Staff Office (S/SO) IT service organizations into a single, agency-wide entity, branded "GSA IT," headed by the Chief Information Officer (CIO). The GSA Office of the Chief Information Security Officer (OCISO) reflects this consolidation. This consolidated information security approach will allow GSA to build on its strengths while minimizing weaknesses and gaps in security. When the consolidation of all GSA IT functions is fully completed, GSA will approach information security and privacy management with an enterprise focus.

The OCISO is organized with an enterprise-wide approach to IT Security operations with services delivered through five distinct security divisions.

- The Staff Office Information System Security Office (ISSO) Division, and Services ISSO Division, provide ISSO and Information System Security Manager (ISSM) support services to consolidated Staff Offices and Service systems. The divisions facilitate integrating IT security in programs and compliance with required security and privacy requirements. ISSOs support their ISSM to their respective division director with a dotted line relationship to other OCISO divisions.
- The Policy and Compliance Division provides management and maintenance of the GSA security authorization, Plan of Action and Milestones (POA&M), Continuous Monitoring, Privacy, and Security Training programs. Further, the Division develops and maintains GSA security policies and procedural guidelines and supports the Federal Risk and Authorization Management Program (FedRAMP) as well as security audit coordination efforts.
- The Security Operations (SecOps) Division provides real-time operational security through the Security Operations Center (SOC) and enterprise network security capabilities. This office manages network security defenses (e.g., intrusion detection system, intrusion prevention system, firewalls, and security incident and event management) and provides automated assessment services including vulnerability scanning and automated penetration testing.
- The Security Engineering (SecEng) Division provides security consulting and engineering support for systems and emerging IT and IT security initiatives. Additionally, it provides incident response and forensic services, manages GSA's Government-wide cloud authorizations, provides manual assessment services including penetration testing, code review, and payment card industry data security standard (PCI DSS) compliance. The division is also responsible for developing and maintaining agency technical guidelines and standards

The GSA develops, manages, and operates a variety of business line applications and general support systems as part of its mission and business functions. These business applications must comply with Federal and GSA laws, regulations, policies, and guidelines.

2.1.1 PURPOSE

The purpose of this effort is to acquire security operations, security engineering, policy and compliance, assessment and authorization, and ISSO support to provide centralized IT security and privacy program services for the GSA through the OCISO. The contractor shall provide IT security technology support and provide independent assessments and recommendations of the GSA IT infrastructures, policies, and procedures.

GSA must comply with the Federal Information Security Management Act (FISMA), Presidential Decision Directives (PDD) 62 and 67, Homeland Security Presidential Directive (HSPD) 7 & 12, and various Office of Management and Budget (OMB) Circulars (e.g., A-123, A-127 and A-130) to ensure critical and sensitive information and infrastructure are adequately protected and continuity of operations are assured.

Additionally, Federal security requirements and guidelines are included in the following publications, which are linked below:

- NIST 800-18 http://go.usa.gov/8CzR
- NIST 800-34 http://go.usa.gov/8Cu3
- NIST 800-37 http://go.usa.gov/8Cum
- NIST 800-47 http://go.usa.gov/8CJB
- NIST 800-53 http://go.usa.gov/8CJe
- FIPS 199 http://go.usa.gov/8CSH
- FIPS 200 http://go.usa.gov/8Ch4

GSA security requirements and guidelines and future updates are also applicable to the requirements of this Order. Current versions are included in Section 9 – List of Attachments as attachments:

- GSA Procedural Guide: Managing Enterprise Risk: Security Assessment and Authorization (CA, PL & RA) (CIO IT Security 06-30) Rev. 7 - 05/31/2011
- GSA Procedural Guide: Plan of Action and Milestones (POA&M) (CIO-IT Security-09-44) - 11/03/2010 Rev. 1
- PCI DSS Requirements and Security Assessment Procedures Version 3.0 – October 2010
- GSA Procedural Guide: Conducting Penetration Test Exercise Guide (CIO IT Security 11-51) Rev 1. - 4/30/2012
- GSA IT Security Policy (GSA Order P. 2100.1I) – 09/19/2013
- GSA Procedural Guide: Continuous Monitoring (CIO IT Security 12-66) – 11/13/2012

As these and any other or additional Federal or GSA security requirements or guidelines are approved, cancelled, implemented, or otherwise changed, the contractor shall comply with these policies, or provide the Government a plan to comply with the requirements and guidelines.

2.1.2 AGENCY MISSION

The OCISO staff has a mission to provide oversight of the agency's IT security program. This

includes the systems operated by GSA to execute its primary missions in serving the taxpayers.

2.2 SCOPE

Under the scope of the TO, the contractor shall provide support to the OCISO security program to manage the security compliance program of GSA applications and support systems. This contract is intended to be the primary resource for the OCISO IT security, Assessment and Authorization (A&A) activities, and FISMA and OMB reporting requirements. This includes acting as a liaison, providing stakeholder communication, providing advice, and making recommendations to the various application and support system program management teams. These services are required to ensure that GSA remains compliant with current and future Federal IT Security requirements.

2.3 CURRENT INFORMATION TECHNOLOGY (IT)/NETWORK ENVIRONMENT

GSA currently has approximately 120 FISMA IT systems. These systems are diverse, and include both Government-Off-The-Shelf (GOTS) and Commercial-Off-The-Shelf (COTS) application systems, which have often been tailored to meet the Government's requirements.

These systems are governed by a variety of management controls, including Investment Review Boards (IRB) and Change Control Boards (CCB).

2.4 OBJECTIVE

The objective of this TO is to successfully provide services to support the security of all GSA IT systems. The contractor shall support all aspects of GSA's information security objectives.

This TO seeks to detect and prevent intrusions, and transition GSA to an increasingly automated scanning and vulnerability mitigation posture with a comprehensive and innovative security engineering solutions to emerging security challenges.

2.5 TASKS

2.5.1 TASK 1 – PROVIDE PROGRAM MANAGEMENT

The contractor shall provide program management support under this TO. This includes the management and oversight of all activities performed by contractor personnel, including subcontractors, to satisfy the requirements identified in this Statement of Work (SOW). The contractor shall identify a Program Manager (PM) by name who shall provide management, direction, administration, quality control, and leadership of the execution of this TO.

2.5.1.1 SUBTASK 1 – COORDINATE A PROJECT KICK-OFF MEETING

The contractor shall schedule and coordinate a Project Kick-Off Meeting at the location approved by the Government. The meeting will provide an introduction between the contractor personnel and Government personnel who will be involved with the TO. The meeting will provide the opportunity to discuss technical, management, and security issues, and travel authorization and reporting procedures. At a minimum, the attendees shall include Key contractor Personnel, representatives from the directorates, other relevant Government personnel, and the FEDSIM COR. The contractor shall provide the following at the Kick-Off Meeting:

a. Transition-In Plan
b. Draft Project Management Plan (PMP)

2.5.1.2 SUBTASK 2 – PREPARE A MONTHLY STATUS REPORT (MSR)

The contractor PM shall develop and provide an MSR (Section 9 - List of Attachments, Attachment B) using Microsoft (MS) Office Suite applications, by the tenth of each month via electronic mail to the Technical Point of Contact (TPOC) and the COR. The MSR shall include the following:

a. Activities during reporting period, by task (include: on-going activities, new activities, activities completed; progress to date on all above mentioned activities). Start each section with a brief description of the task.
b. Problems and corrective actions taken. Also include issues or concerns and proposed resolutions to address them.
c. Personnel gains, losses, and status (security clearance, etc.).
d. Government actions required.
e. Schedule (show major tasks, milestones, and deliverables; planned and actual start and completion dates for each).
f. Summary of trips taken, conferences attended, etc. (attach trip reports to this MSR for reporting period).
g. Accumulated invoiced cost for each CLIN up to the previous month.
h. Projected cost of each CLIN for the current month.

2.5.1.3 SUBTASK 3 – PREPARE A PROJECT MANAGEMENT PLAN (PMP)

The contractor shall document all support requirements in a PMP. The PMP shall:

a. Describe the proposed management approach.
b. Contain detailed Standard Operating Procedures (SOPs) for all tasks.
c. Include milestones, tasks, and subtasks required in this TO.
d. Provide for an overall Work Breakdown Structure (WBS) and associated responsibilities and partnerships between Government organizations.
e. Include the contractor's Quality Assurance Plan (QAP).
f. Include a draft Integrated Master Schedule (IMS) to be further developed in conjunction with the Government to manage milestones and deliverables for all tasks in the Statement of Work. Update the IMS as the schedule changes and once a month at minimum.
g. Be updated on a semiannual basis at minimum or when major changes occur.

The contractor shall provide the Government with a draft PMP on which the Government will make comments. The final PMP shall incorporate the Government's comments.

2.5.2 TASK 2 – PROVIDE AND EXECUTE TRANSITION-IN PLAN

The contractor shall provide a draft Transition-In Plan at the Program Kick-Off. The Plan shall articulate as needed:

a. The contractor's transition approach, process and timelines.
b. The contractor's approach to mitigating or minimizing disruption.

c. The contractor's staffing status.
d. Transition risk management and mitigation strategy.
e. Initial coordination with prior contractor.
f. Gap analysis of required skills.
g. Training approach/knowledge transfer approach.

The contractor shall execute its Government-approved Transition-In Plan. As part of this Plan, the contractor shall ensure that there will be minimum service disruption to vital Government business and no service degradation during and after transition. All transition activities will be completed 30 calendar days after the Project Kick-Off Meeting.

2.5.3 TASK 3 – PROVIDE AND EXECUTE TRANSITION-OUT PLAN

The contractor shall provide a draft Transition-Out Plan at the Program Kick-Off. The plan shall be updated at minimum after the exercise of each option period. The contractor shall finalize and implement its Government-approved Transition-Out Plan 90 calendar days prior to expiration of the TO. The Transition-Out shall provide a seamless transition to the new provider of these services at the expiration of the TO. This includes a concerted effort to ensure full knowledge transfer of the Government's requirements, processes, and institutional knowledge.

2.5.4 TASK 4 – SECURITY OPERATION DIVISION SUPPORT- VULNERABILITY AND CONFIGURATION SCANNING SERVICES

The Government requires an array of holistic and integrated scanning to support maintaining a secure perimeter around the GSA Point of Presence, as well as to ensure applications are secure. Vulnerability discovery is the process of testing and probing the system entry points for flaws that can be used to generate an error condition, raise an invalid response, monitor traffic or data, or control a key system process. Vulnerability and configuration scanning services will allow assessors to determine whether vulnerabilities can be exploited or exposed to violate system boundaries or controls. These vulnerabilities may manifest themselves in several ways such as business process, business logic or design flaws, development errors, or configuration flaws.

2.5.4.1 SUBTASK 1 - QUARTERLY WIRELESS SCANNING

The contractor shall perform quarterly wireless scans for up to five Government buildings in the Washington, D.C., metro area. These tests are to determine unauthorized and insecure wireless access points and ad-hoc networks in these buildings. Buildings are 2-11 stories high. Government locations may change during the performance of this Order; however, the anticipated level of scanning activities is not anticipated to change.

The analysis must include the 802.11a, b, g and n standards. Identified (GSA) Access Points and Peer-to-Peer networks must be checked for compliance with the GSA standard. Differentiation between WEP, WPA, and WPA2 networks shall be noted in the report. The reviews will be conducted using GSA-approved standalone tools or enterprise wireless network monitoring tools.

Access points must be catalogued and addressed in a central data repository to be provided by the GSA, known hereafter as the GSA Project Folder. The contractor shall make contact with and provide counsel as needed to local system administrators of these networks to determine

and/or ensure compliance.

All vulnerability reports shall be posted in the GSA Project Folder. There will be four reviews annually and they shall commence in May, August, November, and February.

2.5.4.2 SUBTASK 2 - WAR DIALING PENETRATION TESTING

The contractor shall provide War Dialing Penetration Testing. Intrusions can occur through the use of dial-up connections to controlled systems. The use of Voice Over Internet Protocol (VOIP) services makes this threat especially pronounced in large organizations. War Dialing Penetration Tests seek to identify if an attacker is able to gain access to the network environment through unauthorized modems and devices.

The contractor shall conduct annual telephone war dialing by using automated tools to identify and connect to GSA modems. The contractor shall ensure that all of GSA's approximately 60,000 phone numbers are scanned to discover modems with no passwords and easily cracked passwords as well as insecurely connected modems.

All vulnerabilities discovered shall be manually verified to determine compliance with GSA guidelines. Vulnerabilities shall be sent to the proper GSA security manager for mitigation.

The Government currently uses Nitcool Phonesweep for war dialing. The contractor may analyze the market and recommend alternative approaches and tools for Government approval should such alternative approaches provide benefit to the Government.

2.5.4.3 SUBTASK 3 - VULNERABILITY AND CONFIGURATION SCANNING (GENERAL OPERATING SYSTEM (OS)/NETWORK LEVEL)

Vulnerability and Configuration Scanning involves maintaining and configuring the regular (weekly) configuration management and vulnerability scans, reviewing the results, and configuring and tuning the configuration management and scan policies.

The contractor shall analyze approximately 45,000 IPs spread across three CIDR/16 networks plus some smaller networks on a weekly basis. These networks and devices are spread between 20-25 services, staff offices, and regions (S/SO/R). The contractor must survey to identify any servers that are not included in existing system inventories and ensure that they are included in subsequent vulnerability review and analysis. Contractor survey techniques must distinguish between servers, workstations, printers, network equipment, and other devices.

The contractor shall monitor sources such as the American Registry for Internet Numbers (ARIN) to identify GSA-assigned networks. These network assignments shall be catalogued and monitored for changes and reported to the Director of Security Operations. The contractor shall verify that networks are indeed assigned to GSA.

The contractor shall survey these networks for servers and services weekly or more frequently, and it shall conduct unauthenticated scans against identified servers and services.

The contractor shall conduct authenticated vulnerability scanning weekly or more frequent for approximately 5,000 servers, 2,000 network devices, and 2,000 printers and other devices. The

total number of devices requiring authenticated scans is expected to slowly increase over time but is not expected to exceed 10,000 devices.

The contractor shall coordinate and obtain the required permissions and scan credentials for authenticated scans. If access is not granted by the system owner or scan results cannot be obtained, the contractor shall notify the COR and Technical Point of Contact (TPOC) within five days for resolution.

The contractor shall ensure that all current and newly added servers, network devices, and printer/copiers have been mapped to the FISMA-assigned system and a point of contact has been determined. The contractor shall interface with applicable ISSMs and ISSOs, surveying them on a monthly basis to determine any additional systems that need to be scanned that are not discovered via automated tools.

The contractor shall establish and maintain accounts in the GSA Vulnerability Manager for the ISSMs/ISSOs and technical designees in the 20-25 S/SO/R to review scan results and/or perform its own scanning. These accounts shall be set up and maintained throughout the year. The contractor shall recertify users' access to the system annually.

The contractor shall update and maintain an IT Security Scanning procedures document that describes the scanning process and the roles and responsibilities of the individuals involved in the scanning process. This document shall be updated bi-annually at a minimum and whenever there are major changes in the procedures.

Scanning must be capable of producing Common Vulnerabilities and Exposures (CVE), Common Configuration Enumeration (CCE), and Common Platform Enumeration (CPE) output. Configuration scans shall be run using Security Content Automation Protocol (SCAP) content provided by the GSA Security Engineering Team. The contractor shall configure the SCAP policy files to support the requirements of the GSA-provided tools. GSA exceptions to standard policies, such as CIS or the Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIG), should be managed either within the tool or in the SCAP files themselves. Scans shall be conducted and produce Cyberscope compliant output. The contractor shall assist the Government in uploading the output files to the cognizant Government agencies.

The contractor shall determine which vulnerabilities are applicable to the GSA environment and only forward those on for mitigation and inclusion in the Assessment and Authorization (A&A process. False positives and non applicable vulnerabilities must be reduced to the greatest extent possible, marked as such within the GSA Vulnerability Manager, and documented as appropriate.

The contractor shall provide the various S/SO/Rs support to answer and/or resolve questions about potential false positives, and determine if the vulnerability is applicable in each situation. The contractor shall provide instructions and assistance in mitigating the vulnerabilities discovered via email and phone as needed.

The contractor shall use GSA internally accessible documentation and tools (such as IP Address management tools, spreadsheets, and notes) and the GSA ISSM and ISSO contact list to determine which IPs to send to which security managers for mitigation.

The contractor shall use the scanning process document noted above for the notification and reporting process. Reports are managed through the GSA Vulnerability Management tool and may be automated. Vulnerability reports and raw data may be requested to be posted in the GSA Project Folder.

Network & OS Scanning Tool Management

GSA currently uses the following tools for vulnerability scanning and testing of servers:

a. Tripwire IP360 (Also some use of Tenable Nessus/SecurityCenter)
b. Tripwire CCM
c. Tripwire SIH
d. Metasploit Pro
e. CORE Impact, CORE Insight

The contractor shall, upon Government request, evaluate new scan tools. This includes researching technologies using the internet and other sources of public information, as well as meeting with potential providers of tools to further explore suitability to the Government's requirements.

The contractor shall manage and maintain the GSA Vulnerability Management tools, including Structured Query Language (SQL) server tuning and maintenance, backups, OS maintenance, and troubleshooting.

Training

The contractor shall develop and provide one-hour training sessions as needed based on the scanning process. This training session shall be focused towards the end users of the scan tools (primarily ISSOs and ISSMs) and will be held up to four times annually. The training sessions will be recorded for later playback by internal GSA end users.

2.5.4.4 SUBTASK 4 - VULNERABILITY SCANNING (WEB APPLICATIONS)

GSA serves a myriad of unique stakeholders across both the private and public sector through interactive web applications. In order to ensure that these web-based applications are secure, the Government requires scanning to ensure all potential security vulnerabilities and architectural weaknesses are remediated.

The contractor shall perform approximately 40-50 authenticated scans per month in addition to 110 firewall web server scans per year as noted in Task 2.5.6.3, Firewall Change Request Processing. There will be approximately 400 additional unauthenticated web applications scans per month that must be configured and maintained in the enterprise web application scan tool console (currently HP AMP) and the GSA Vulnerability Manager (currently Tripwire) as well as 150 authenticated scans per year using the enterprise web application scan tool. At the Government's discretion, the tool used for unauthenticated scanning shall be migrated from HP AMP to Tripwire Web360 or similar tool within two months of requesting this. At the government's discretion, the tool used for authenticated scanning shall be migrated from HP AMP to a different enterprise scan tool (such as HP's SSC and WebInspect Enterprise) within 2 months of requesting this.

The contractor shall ensure that reports are provided to the appropriate system owners, ISSMs and ISSOs within two business days of the scans being completed (this may be automated), and conduct a monthly call with developers and system administrators from each SSO to discuss questions or concerns they may have with the scan results or process. The contractor shall maintain statistics of scans, false positives, accepted risks and known vulnerabilities and vulnerability age in a separate spreadsheet.

The Government will provide inventories, necessary access and permission to scan the systems, and assist as needed in mitigation of vulnerabilities found during the analysis.

Tools:
GSA currently uses the following tools for web application scanning, and vulnerability scanning which shall be maintained by the contractor:

a. HP WebInspect (migrating to HP WebInspect Enterprise)
b. HP AMP (migrating to HP SSC)
c. nCircle WebApp 360

2.5.4.5 SUBTASK 5 - VULNERABILITY AND CONFIGURATION SCANNING (DATABASE)

The contractor shall conduct vulnerability analysis of GSA databases. These databases shall be analyzed for compliance to the GSA Hardening Guide and for well known vulnerabilities using the GSA Vulnerability Manager. The contractor shall perform approximately 1,000 authenticated database scans per month. The contractor shall ensure that Database Vulnerability Reports, which are the results from the scans, are provided to the appropriate system owners, ISSMs and ISSOs within two business days of the scans completed (this may be automated).

The contractor shall be responsible for gathering and maintaining the inventory from various GSA sources and contacts. The Government shall ensure that necessary access to the databases is provided.

Tools:
GSA currently uses nCircle CCM (and occasionally AppSecInc DBProtect) as its Vulnerability Manager. The GSA Vulnerability Manager shall be maintained by the contractor. Assistance will be provided by the GSA server services team for domain, OS, and hardware maintenance as needed.

2.5.5 TASK 5 – SECURITY ENGINEERING

Security engineering ensures multiple software components, hardware components, communication components, and processes and integration components across a project are designed and implemented to create a single functioning system that can deliver the business functionality proposed. IT security is embedded and threaded throughout the IT architecture for a project. A multi-disciplinary approach is required to ensure appropriate IT security is implemented and that IT systems function as single units.

2.5.5.1 SUBTASK 1 - DEVELOP AND MAINTAIN GSA HARDENING GUIDES AND APPLICATION BENCHMARKS

The contractor shall develop and maintain GSA hardening guides. These guides shall leverage existing GSA hardening guides, comply with NIST guidelines, and utilize the best practices from with the Center for Internet Security Benchmarks (Level I) and industry.

The contractor shall develop, maintain, update, and test GSA application benchmarks. These benchmarks shall identify performance standards for compliance with the Government-approved GSA hardening guides.

The benchmarks shall include developing or updating security hardening guides including the supporting template files and batch files (as necessary) and SCAP content (security checklists) and testing the associated GSA images. Guides and supporting SCAP content must be compliant with GSA tools including nCircle and MaaS360. SCAP content must align with GSA requirements (i.e., must be modified to account for GSA exceptions and/or policy requirements that are unique to the agency). SCAP content must map to CCEs, CVE, CPEs, XCCDF and OVAL formats.

The contractor shall provide assistance to GSA Information System Security Officers and the OCISO Security Operations Division in the application of benchmarks, including troubleshooting the implementation of required benchmarks for information systems and making appropriate changes to the GSA benchmarks, as needed. Further, the contractor shall coordinate with the OCISO Security Operations Division which is responsible for performing automated reviews against SCAP benchmarks to ensure any issues resulting from configuration errors in benchmarks are appropriately remediated.

Below is the current list of guides and benchmarks which need to be developed and maintained. New guides and benchmarks will need to be developed as the GSA application standards change. For all guides and benchmarks, there will be approximately one update to the hardening guide annually, and the contractor shall ensure the guides are kept current.

Develop New Guides and SCAP content

a. Windows 2012
b. Solaris 9
c. Solaris 10
d. Oracle 11G
e. MySQL 5.0
f. RedHat Linux 6
g. MS SQL Server 2008 R2
h. MSSQL Server 2012
i. MS IIS 8
j. Apache 2.4
k. Sybase IQ 16

Update Existing Guide

a. Windows 7 (USGCB SCAP content exists)
b. Windows 2003 (GSA customized SCAP content not available)
c. Windows 2008 (GSA customized SCAP content not available)
d. Windows 2008 R2 (GSA customized SCAP content not available)
e. MS SQL Server 2008 (GSA customized SCAP content not available)

2.5.5.2 SUBTASK 2 – DESKTOP SOFTWARE TESTING

The contractor shall test new desktop software including, but not limited to, Chrome Extensions, for vulnerabilities and present recommendations for usage within GSA. The contractor shall perform automated and manual security testing and analysis on all proposed new desktop software.

The contractor shall develop, update, and maintain desktop software testing process documents that describe the desktop software testing process, usage of tools, development of resultant testing reports with recommendations for usage within GSA, and the roles and responsibilities of the individuals involved in the testing. This document shall be updated whenever there are major changes in the process and/or bi-annually.

As with all major changes, the contractor shall be required to present this documentation, as well as documentation of the impact to the agency to the applicable CCB or approving authority.

2.5.5.3 SUBTASK 3 – SECURITY CONSULTING AND ENGINEERING SUPPORT

The contractor shall work closely with ISSOs, ISSMs, system program managers, and supporting development teams to ensure GSA applications and systems are securely architected and meet or exceed GSA security standards and requirements. Focus will be on system and application development efforts in the initiation and development phases and on systems in the implementation phases undergoing major changes to ensure systems are securely designed and implemented before they go into operation.

The contractor shall ensure multiple software, hardware, communications, process, and integration components across a project are designed and implemented to create a single functioning system that can securely deliver the business functionality proposed. It is incumbent on the contractor to utilize a multidisciplinary approach in order to ensure that IT security is embedded throughout the IT architecture. The contractor shall be prepared to design, develop, and integrate interfaces that could be either software or processes in order to resolve highly complicated and evolving IT security issues faced by GSA.

In addition, the contractor shall provide technical expertise and advice on the restructuring and/or re-architecting of major Government networks to ensure the best secure placement and configuration of network tools and appliances in order to provide the maximum protection of various types of sensitive Government data.

The Government estimates that each security engineering and consulting support project will have a three to six-month life cycle. These projects tend to have short lead times and varying knowledge requirements. The contractor shall acquire the necessary skill sets and subject matter expertise to fulfill the Government's requirements within one month of stated need. The contractor shall provide subject matter expertise in security engineering, system security integration, and security consulting support in the design, implementation, and modification of GSA information systems. The contractor shall support highly technical IT projects dealing in cloud security, virtualization security, web application security, network architecture and active directory design/segmentation, and secure coding, and source code reviews (Java, C++, C#, ASP .NET, VB, APEX, PERL, PHP, RoR, etc).

The contractor shall attend GSA Change Control Board meetings, review and comment on design documents, perform testing as needed, and develop security engineering plans. The contractor shall ensure all GSA requirements are addressed in the development of new applications and when there are major functional and or architectural changes.

The Security Engineering Subject Matter Expert (SME) shall be available to support activities under other tasks, particularly Tier 3 incident handling/forensics staff, when necessary.

The contractor shall support the following types of application/network systems, which are representative but not inclusive of the types of support required:

a. Building Control systems / Physical Access Controls
b. Mobile Device Security
c. Cloud-based information systems leveraging Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS)
d. Data Integration and Analysis Systems
e. Enterprise Single Sign On / Multi-Factor Authentication Solutions

2.5.5.4 SUBTASK 4 – INCIDENT MANAGEMENT AND RESPONSE

GSA has a formalized Incident Response program including forensics capabilities that are supported by policies, procedures, supporting processes, and enterprise tools. The GSA Incident Response program, although focused largely on GSA IT resources, also serves as the Incident Response coordinator for incidents involving GSA vendor-owned/operated information systems that have been authorized to operate by GSA, and reports incidents to United States – Computer Emergency Readiness Team (US-CERT) and law enforcement as necessary.

GSA receives threat information from the following sources:

DHS, US-CERT, National CyberSecurity and Communications Integration Center

a. Joint Indicator Bulletin (JIB) - Malware indicators, network traffic, tool indicators, hostnames, and IP addresses known to be associated with the ongoing malicious activity.

b. CISCP Indicator Bulletin (CIB) - Attack descriptions (e.g., phishing, malware) with indicators of compromise (URLs, Intrusion Prevention System [IPS], MD5s).

c. Security Awareness Report (SAR) - General security awareness including malware analysis, Indicators of Compromise (IOCs), Uniform Resource Locators (URLs), Fully Qualified Domain Names (FQDNs), QDNs, Domains, MD5s.

d. Malware Initial Findings Report (MIFR) - Malware analysis with indicators of compromise (e.g., Name, Type, Size, MD5, Packers, Sections).

e. Early Warning and Indicator Notice (EWIN) - General cyber threat info including IOCs.

f. Industrial Control System Cyber Emergency Response Team (ICS-CERT) Alerts/Advisories - General cyber threat info including IOCs related to Industrial Control Systems.

g. WILLHACK Notes - General security awareness and trends for Industrial Control Systems and Intel feeds (chatter).

h. Malware Analysis Report (MAR) - Malware reverse engineering report with IOCs.

i. Technical Information Paper (TIP) - High-level discussion of security technology.

j. Joint Security Awareness Report (JSAR) - General cyberthreat information and analysis with IOCs.

k. US-CERT Advisory - General cyberthreat information and analysis with IOCs.

l. Weekly Analytic Synopsis Product - Weekly synopsis of global cyberthreats, including trending.

m. US-CERT NCCIC - Specific, actionable threat information that describes real-time compromise of GSA systems; data is often times from E2 and includes PCAP.

n. ThreatScape / iSIGHT Partners Vulnerability and Threat Reports - Threat, exploit, and vulnerability analysis with indicators of compromise.

GSA receives actionable incident alerts from contracted managed security services, GSA enterprise security tools, and external sources:

a. Managed Security Services

1. CenturyLink Security Operations Center (GSA MTIPS (Intrusion Prevention System) Provider) - Specific, actionable information about GSA hosts potentially engaged in behavior consistent with malware (not necessarily Advanced Persistent Threat (APT)).
2. Verizon Security Operations Center - Specific, actionable information about GSA hosts potentially engaged in behavior consistent with malware (not necessarily APT).
3. Mandiant Network Threat Assessment Program (NTAP) Alerts - Specific, actionable threat information that describes real-time compromise of GSA system by APT malware.

b. GSA Enterprise Security Tools

1. **McAfee Enterprise Security Manager (aka Nitro) -** The Security Incident and Event Management (SIEM) Tool that collects and correlates event log data from network devices across the network including Firewalls, IDP/IPS devices, Web Proxies, and Wireless Access Points.
2. **MIR: Mandiant Intelligent Response -** An appliance-based solution that allows security analysts to perform real-time network sweeps and forensic analysis of workstations and servers to detect APT malware.
3. **Bit9** - Deployed as an application white listing solution that identifies executables on GSA workstations/servers in a central repository for investigation into whether malware was executed on a device.
4. **Palo Alto Wildfire** - Cloud-based malware detection service which performs static and dynamic analysis of binary executables ingressing GSA network. Alerts on detection of malware.
5. McAfee Nitro Security IPS (Intrusion Prevention System)

c. Incident Alerting from External sources

1. DHS/NCCIC
2. Federal Bureau of Investigations
3. GSA Office of Inspector General
4. Other Law Enforcement
5. Public

GSA currently uses the enterprise security tools identified above as well as the following enterprise solutions to investigate security incidents:

a. **NetIQ** - Identity Management Tool used for correlating VPN identifiers to users.

b. **McAfee ePO -** ePo provides centralized event collection and reporting for McAfee antivirus software on GSA workstations and servers. It allows security analysts to investigate malware incidents and trends.

c. **MaaS360 -** The software management tool that GSA uses to deploy and inventory software on workstations and mobile devices.

d. **Mandiant MCIRT Portal** - Allows for access to alerts from Mandiant regarding threats

e. **Verizon Security Operations Center (SOC) Portal** - Allows for access to alerts from the Verizon Security Operations Center.

f. **CenturyLink Portal** - Allows for access to alerts from the CenturyLink Security Operations Center.

g. **iSight Portal** - Allows for access to ThreatScape / iSIGHT Partners Vulnerability and Threat Reports.

h. **nCircle** - Used to identify exposure to vulnerabilities in GSA systems.

The contractor shall provide incident response and forensics support to the GSA at the agency-wide level. This support shall be focused on analyzing security threat information from a myriad of internal and external threat sources, GSA contracted managed security services, and GSA enterprise security tools; verifying GSA exposure (if any); and mounting effective cyber response. Further, the contractor shall provide incident response support for all incidents reported to the OCISO from incident initiation to incident closure consistent with GSA Incident Response Procedures documented in GSA IT Security Procedural Guide 01-02, *Incident Response*. Incident support must include third tier incident handling for major/complex incidents involving APTs, special investigations, and/or incidents requiring digital forensics.

All evidentiary data involving incident investigations shall be securely handled and ensure chain of custody in accordance with GSA policy.

Incident analysis and response to alerts received during business hours (7:00 AM – 6:00 PM Eastern Time (ET)) shall be initiated immediately. During non-business hours, the contractor shall respond to incidents as follows:

1. Critical Incidents - response within one hour
2. Important Incidents - response within four hours

3. Routine Incidents - Can be handled during next business day

The contractor shall travel to an incident scene as necessary to support an on-site incident investigation.

The contractor shall provide malware investigation, leveraging a combination of open source, commercial, and cloud-based tools to perform both static and dynamic analysis. The results of the analysis shall be used to develop IOCs which are subsequently used to look for similar instances of malware. Further, the analysis shall attempt to reveal the identity of the malicious actors, their intent, and provide guidelines for protecting against subsequent attack.

The contractor shall utilize GSA's enterprise security tools to investigate security incidents. This includes creating and maintaining the alerts within these tools, analyzing the data captured, and reporting the data as appropriate to the Government stakeholders.

The contractor shall maintain the Mandiant Intelligent Response (MIR) controllers (two devices, provided as Government Furnished Property (GFP)). Maintenance is limited to software upgrades as applicable and development and updates of IOCs in coordination with the supporting vendor.

The contractor shall update and maintain incident management process documents that describe the analysis of cyber threat information, the incident report and response process, and the roles and responsibilities of the individuals involved in it. This document shall be updated at least every six months or after major IT security incidents.

The contractor shall report any security incidents per GSA/Federal policy, and assist and coordinate security events with other GSA stakeholders. The Government anticipates the following frequency of incidents:

Routine / Important Incident Frequency

- 20-25 alerts daily - Bit9, Nitro SIEM, WildFire, Verizon SOC, CenturyLink SOC, and other threat sources- Follow-up based on continuous monitoring alerts and initiate appropriate response, remediation, and reporting actions.

Critical Incident Frequency

- 12 Mandiant NTAP alerts requiring investigation annually
- 12 US-CERT/NCCIC/FBI reports requiring investigation annually
- 3-5 Major incidents annually requiring forensic analysis

2.5.5.5 SUBTASK 5 – MANUAL PENETRATION TESTING

The contractor shall provide penetration testing support in order to demonstrate the exploitability of identified problems and findings which may not be readily apparent when performing an automated security review. The contractor shall perform "Gray Box" penetration testing with minimal insider knowledge of the system. The assessment, although usually externally focused, may be internal, or both. Gray Box testing involves the execution of a scenario or abuse case that focuses on violating technical, administrative, and management controls in the system. Penetration testing activities shall be in compliance with requirements in GSA IT Security Procedural Guide, CIO-IT 11-51: Conducting Penetration Testing, which is attached in Section 9

– List of Attachments, Attachment P.

The contractor shall leverage existing vulnerability information available via GSA enterprise security tools or prior assessment data to facilitate the assessment. The focus of the penetration testing must be to identify possible systems weaknesses NOT found via common vulnerability scanning tools. The exercise should be designed to take a comprehensive view of production resources to identify non-obvious gaps, loopholes, or process circumvention techniques and test business rules/logic that can be leveraged to penetrate GSA information systems.

The contractor shall create a test plan including the rules of engagement consistent with GSA Guide requirements and submit to the GSA for review and approval prior to commencement of testing activities.

The contractor shall create a Penetration Test Report consistent with the requirements in GSA IT Security Procedural Guide, CIO-IT 11-51: Conducting Penetration Testing.

The GSA expects that 15 to 30 penetration tests will be required annually. Historical data indicates testing has averaged 40 hours per test.

2.5.5.6 SUBTASK 6 – SOFTWARE CODE REVIEW

The contractor shall perform malware analysis and software code review using GSA provided automated code review software. The contractor staff shall have knowledge in web application security, secure coding, and source coding in a number of programming languages (Java, C++, C#, ASP .NET, VB, APEX, PERL, PHP, RoR, etc). The contractor must be able to quantify and analyze results and provide support to programmers for making corrections to the code, not just running automated scans and presenting the resultant scan report. Additionally, the contractor shall be required to review and at Government's request provide a short, high level analysis of program documentation.

The contractor shall ensure that FISMA information systems required to undergo code review are defined within the respective code review tools. The contractor shall be required to interface with applicable ISSMs and ISSOs, surveying periodically to determine if there are additional systems that need to be scanned and setting them up in the respective code review tools. The contractor shall work with system owners to obtain access to code required for review.

The contractor shall maintain the GSA Fortify/SSC and CheckMarx application stack; servers are managed centrally by another contractor organization. Maintenance is limited to software upgrades, as applicable, in coordination with the supporting vendor.

The contractor shall develop, update and maintain Software Code Review process documents that describe the GSA software code review program, software code review process, use of the tools, analysis of the resultant code review reports, and the roles and responsibilities of the individuals involved in it. This document shall be updated whenever there are changes in the process and/or bi-annually.

The contractor shall use the software code review process documents (to be developed) to facilitate the notification and reporting of identified vulnerabilities to Government stakeholders.

The contractor shall, upon Government request, evaluate new code analysis tools. This includes researching technologies using the internet and other sources of public information, as well as meeting with potential providers of tools to further explore suitability to the Government's

requirements.

The contractor shall maintain and hold training sessions as needed based on the code review scanning process. Training shall be focused towards the end users/developers and system program managers and may be recorded for later playback by internal GSA end users. Training sessions shall be approximately 30-60 minutes and held at most four times per year.

The GSA expects to perform an estimated 100-150 automated source code scans annually together with resultant result analysis (some source code review) to minimize false positives and recommend code fixes to system developers and programmers. The contractor shall also assist developers with configuring their tools so that the developers can run their own automated source code scans.

Tools:
GSA currently uses CheckMarx for mobile code analysis and Fortify for static code; both are GFP. The contractor shall maintain the servers supporting the automated software code review.

2.5.6 TASK 6 – SECURITY OPERATIONS

The SecOps Division supports a broad array of security services. This includes:

a. Security Information and Event Management (SIEM) and SOC Monitoring and Analysis
b. Application Whitelisting Management
c. Firewall Change Management
d. Security Consulting and Engineering Support
e. Hardening Guide and Application Benchmark Management
f. Penetration Testing
g. Network Audits

This also includes scanning and testing vulnerability and configuration scanning; manual verification using penetration test tools and methods; management of the scanning infrastructure to include appliances, servers, and databases; and configuration of command line scripts to support the scanning infrastructure and vulnerability scanning process.

2.5.6.1 SUBTASK 1 - SIEM AND SOC MONITORING AND ANALYSIS

The GSA SIEM tool currently processes approximately one billion raw events per day that with tuning, consist of 20-40 actionable events per week.

The contractor shall provide support for general daytime/weekday monitoring of events within the SIEM tool as defined below.

The contractor shall create and manage correlation rules within the tool in order to automate blocking of known bad traffic; blacklisting hosts that are conducting malicious activity while taking care to not blacklist or block any legitimate traffic. The contractor shall also create and maintain correlation rules that flag interesting possible malicious traffic that needs further inspection. These events might be routed to other divisions or external 24/7 security operations centers (e.g., MTIPS or Networx). The contractor shall tune IDS/IPS systems by suggesting and implementing changes to which rules are enabled or disabled. The contractor shall balance a secure environment where significant events are not missed, with a functional IDS/IPS/SIEM

tool.

The contractor shall respond to detected threats by analyzing security alert data, performing high level malware and/or software analysis. The contractor shall monitor for high risk alerts, events and correlation events created by the SIEM tool and respond within a period of four business hours from the time of occurrence. Less significant events shall be marked as such. Responses range from, and may include, initiating additional manual blocking or flagging events to the Security Engineering Incident Response team for further incident analysis.

The contractor shall create a weekly review of the noteworthy audit log events collected through this tool and from the SOCs and any actions taken.

The contractor shall create and keep updated a process and procedure document for this subtask.

The contractor shall provide standby, on-call support 24x7x365, to address critical network events as needed. (Actual off-business hour events are estimated to be less than one to two per week.) This includes having at least one member of staff familiar with the suite of GSA Security Operations tools available at all times to respond to calls or texts/pages for support. Critical events shall be reported, using existing Standard Operating Procedures (SOP) within one hour. Other alerts reporting shall occur 8:00 AM to 5:00 PM ET Monday through Friday. Contractor personnel shall work with GSA Government personnel and other contractor teams on the resolution of all NIDS/NIPS alerts.

When major changes to network monitoring tools are scheduled and these changes might affect the enterprise, the contractor will need to document the changes, impact to the agency, and applicable testing and present it to the applicable GSA CCBs. These meetings usually occur weekly.

The task of SIEM and SOC monitoring and analysis relies heavily on GSA Information Assurance contracts awarded outside of this TO, and procedures that are already in place. The contractor shall act as a liaison and coordinate its activities with the other support contractors.

a. GSA has a contract in place for the management and overall protection of the SIEM tool and the data that feeds into the SIEM tool.
b. The Government has contracted with SOC operators, Verizon and CenturyLink, and with DHS/US-CERT. The contractor shall act as a liaison to the SOCs

Tools:
The Government currently uses the following GFP tools for SIEM and SOC monitoring Analysis:

a. McAfee (aka Nitrosecurity) SIEM suite
b. SourceFire
c. SNORT
d. ArcSight SIEM installation (this is a legacy installation that the contractor will occasionally interface with and that will be transitioned to the McAfee SIEM suite)

2.5.6.2 SUBTASK 2 – MANAGEMENT OF APPLICATION WHITELISTING PROCESS

The contractor shall manage the Enterprise Application Whitelisting suite. The contractor shall manage the application to include all requirements above the OS itself. This includes, but is not limited to:

a. Hardware performance tuning.
b. SQL server management.
c. Verifying backups.
d. Tuning policies.
e. Managing and maintaining exclusions.
f. Software optimizations.

The contractor shall coordinate with local support, central support and end users to troubleshoot end user issues, as well as coordinate with software and hardware vendors' support operations for troubleshooting white listing server issues.

The contractor shall perform the following routine tasks as prescribed below:

Frequency	Task
Multiple Times Daily	Interact with support staff to facilitate blocking/unblocking of files
Twice Daily	Monitor for legitimate applications that are being blocked. Manage software policies
Daily	Monitor the overall health of the tool; check that backups of the system are successful
Weekly	Status report on system health, block activity and interaction with support staff
Monthly	Ensure patching of the system is up to date. Monthly summary status report of system health, block activity and interaction with support staff
Every 30-60 Days	Test and deploy new versions of the client software to servers and workstations

Tools:
The contractor shall create and maintain documentation of the application white listing tool. GSA currently uses the Bit9 Parity tool.

2.5.6.3 SUBTASK 3 – FIREWALL CHANGE REQUEST PROCESSING

The Contractor shall conduct vulnerability analysis of servers and web applications requesting access through the GSA firewalls. These servers and the applicable firewall change requests shall be analyzed for compliance with the applicable GSA IT Security Procedural Guides using the GSA Vulnerability Manager and Web Application Scanner as well as the GSA penetration testing tool. Historically, the GSA has averaged 110 change requests per year; however GSA expects this number to be between 150 and 200 in the base year. There will also be 20 to 30 internal firewall requests per month to review for soundness and compliance with GSA IT Security Procedural Guides. These internal firewall requests may require that the contractor draft

firewall rules to be provided to other GSA groups or managed SOC vendor for implementation.

The contractor will be required to complete change request processing for perimeter firewalls within five work days, and internal firewall requests within three work days. The contractor shall work with the system administrators and ISSMs/ISSOs to obtain necessary access to the systems, and assist in mitigation of vulnerabilities found during the analysis.

Tools:
GSA currently uses the following tools:

a. Tripwire IP360 (formerly nCircle)
b. HP Webinspect/AMP (moving to HP WebInspect Enterprise and HP SSC)
c. Metasploit Pro
d. CORE Impact
e. Microsoft Baseline Security Analyzer

2.5.6.4 SUBTASK 4 – NETWORK AUDITS

SecOps is also responsible for conducting wireless and wired network audits across the agency. The contractor shall conduct network audits at the request of the Government.

2.5.7 TASK 7 – INFORMATION SYSTEM SECURITY OFFICER SUPPORT

The Government has established two ISSO divisions in the OCISO. The first ISSO Division is the Staff Offices ISSO and the second is the Services ISSO. ISSOs possess the primary responsibility for ensuring compliance with required security and privacy requirements for GSA IT systems under ISSO jurisdiction. The ISSOs in these Divisions provide support to ISSMs and currently have responsibility for 27 distinct information systems of varying size and user groups belonging to system owners across GSA IT. This number may increase or decrease based on agency need and reorganization.

The contractor shall provide support for both OCISO ISSO support Divisions. This support consists of a set of responsibilities that are universal to all GSA IT systems requiring ISSO support.

For its assigned system(s), the contractor shall assist in coordination of services provided by the Security Operations, Security Engineering, and Policy and Compliance Divisions to ensure systems are securely implemented and comply with FISMA, OMB and GSA Policies.

The contractor shall provide support for traditional IT systems, as well as Building Monitoring and Control (BMC) systems including, but not limited to, building technologies such as advanced metering systems (AMS), building automation systems, lighting control systems, physical access control systems (PACS), renewable energy systems, and kiosks. These systems, while closely related to the scope of facilities management, are IT systems, and as such are subject to the same Federal and agency-specific policies and security standards as any other Federal IT system. To support these systems, the contractor must possess highly specialized knowledge of BMC systems, understand the threats they pose to the GSA enterprise network, and be able to provide guidance on securely implementing such systems.

The contractor shall work closely with the OCISO Security Engineering Division, the Services ISSMs, and the PBS Buildings Management System Program Managers to develop a systematic,

repeatable approach to securely implement such systems. The contractor shall facilitate systems assessment and authorization on systems for which the contractor has responsibility. The ISSO shall collaborate with system owners and business lines to remediate identified vulnerabilities, and provide suggestions based on its expertise to manufacturers, vendors, and building managers as to how to resolve vulnerabilities or mitigate threats discovered during the assessment.

These coordination activities shall also include SDLC support, participating in cross-discipline project teams, and working with system owners and business lines in matters concerning the assigned system(s). The contractor shall evaluate assigned information systems to ensure systems are securely hardened, patched, monitored, and evaluated via available assessment services and ascertain if additional safeguards are needed.

The contractor shall ensure all systems are operated, maintained, and disposed of in accordance with documented security policies and procedures. For assigned systems that may be contractor owned and contractor operated, the contractor, in coordination with Government ISSMs, shall ensure that such vendors comply with GSA security and privacy requirements.

The contractor shall provide comprehensive documentation, development, and operational support for GSA IT Security programs for major and minor applications and general support systems. The contractor ISSOs shall act as the primary resource for all IT security documentation development and revision. Documentation requirements include:

a. System security plans
b. Continuous monitoring plans
c. Configuration management plans
d. Contingency plans
e. Contingency plan test reports
f. Plan of action and milestones
g. User recertification
h. FISMA assessment
i. Assessments reflecting customer responsibilities for GSA cloud systems and assessments supporting the limited ATO process for cloud systems
j. Incident reports

The contractor shall advise ISSM, system owners, and OCISO staff in other Security Divisions of risks to assigned systems. The contractor shall research assigned IT security systems to provide insights on IT security architectures and IT security recommendations for assigned systems. The contractor shall serve as the IT Security point of contact for assigned Service and Staff Office systems. The contractor's activities shall be coordinated with other OCISO Security Divisions, as appropriate. The contractor shall provide recommendations which identify how to improve the IT security function to reduce costs, increase quality, and improve response times.

The contractor shall assist in the coordination of services provided by other OCISO Security divisions including Security Operations, Security Engineering, and Policy and Compliance as well as SDLC support, and participate in cross-discipline project teams and work with system owners and business lines.

The contractor shall attend internal Federal Government IT security meetings which may be weekly Divisional meetings, ISSO/ISSM meetings, project meetings, change control, engineering review or other meetings. The contractor shall review and coordinate reporting of Security Advisory Alerts (SAA), compliance reviews, security training, incident reports,

contingency plan testing, and other IT security program issues, and prepare and report on the IT security architecture, IT security processes and IT security posture of supported IT security systems at GSA. The contractor shall manage identification and authentication schemes used in systems as well as new user requests.

The contractor shall prepare incident reports, assist or perform in incident mitigation, and forward incident reports as appropriate (after consultation with the ISSM) to the OCISO SecEng Division for incident management and/or US-CERT reporting.

The contractor shall provide a detailed approach that addresses the functional delivery of the specified tasks listed in the sections below for ISSO support. The contractor shall:

a. Perform as the lead IT security point of contact (POC) for all activities related to IT security for assigned information systems, coordinating activities and services from other OCISO Security Divisions (i.e., SecOps, SecEng, and Policy and Compliance) to ensure systems are securely implemented and operating as intended.
b. Provide oversight and responsibility for implementation of system security and privacy requirements.
c. Coordinate and facilitate across OCISO Security Divisions to ensure available services are implemented for assigned systems; evaluate assigned information systems to ensure systems are securely hardened, patched, monitored, and evaluated via available assessment services; ascertain if additional safeguards are needed; and develop and maintain system security documentation.
d. Oversee and manage relationships for assigned systems that may be contractor owned and contractor operated, ensuring vendors comply with GSA security and privacy requirements.
e. Ensure systems are operated, used, maintained, and disposed of in accordance with documented security policies and procedures. Ensure GSA information systems comply with FISMA, OMB and GSA Policies.
f. Advise ISSM, System Owners, and OCISO staff in other Security Divisions of risks to assigned systems.
g. Research assigned IT security systems to provide insights on IT security architectures and IT security recommendations for assigned systems; activities shall be coordinated with other OCISO Security Divisions, as appropriate.
h. Assist in identifying how to improve the IT security function to reduce costs, increase quality, and improve response times.
i. Serve as the IT Security POC for assigned Service/Staff Office systems, coordinating IT security issues with other OCISO security divisions, as appropriate.
j. Review and coordinate reporting of Security Advisory Alerts, compliance reviews, security training, incident reports, contingency plan testing, and other IT security program issues.
k. Identify, report, and respond to security incidents following GSA Information Security policy and process requirements; security incident reporting and response activities are lead by the OCISO SecEng Division.

2.5.7.1 SUBTASK 1 – VULNERABILITY AND CONFIGURATION MANAGEMENT

The contractor shall coordinate with OCISO security operation division to ensure that the

information system to which they have been assigned responsibility has been correctly identified in vulnerability and configuration assessment and enterprise monitoring systems. Additionally, the contractor shall ensure that assessors are notified of false positives, track vulnerabilities from discovery through remediation, document risk acceptance, and maintain a history of documented changes. Vulnerabilities and mis-configuration derived from automated assessment tools are to be documented in the POA&Ms or managed in automated assessment systems.

The contractor shall utilize available GSA enterprise vulnerability, configuration, and monitoring solutions (including SIEM) to perform log reviews, verify system inventory, ensure systems are configured consistent with agency security benchmarks, are patched to current patch levels, and are securely maintained.

The contractor shall coordinate activities with the SecEng Division to provide basic support for the incorporation of code scanners and analysis tools into GSA's development process.

The contractor shall assess vulnerabilities to ascertain if additional safeguards are needed, ensure systems are patched and security hardened at all levels of the "stack," and monitor to see that vulnerabilities are remediated as appropriate. The contractor shall review system security audit logs locally or via enterprise management systems to ensure security measures are implemented effectively and operating as intended. The contractor shall coordinate non-standard software/hardware through established approval processes.

The contractor shall complete the annual user recertification and user reauthorization, and shall facilitate annual visitor access control re-certifications for Datacenters for systems for which they have responsibility.

The contractor shall complete the annual FISMA assessment and support and implement continuous monitoring as assigned.

2.5.7.2 SUBTASK 2 – SYSTEM DEVELOPMENT LIFECYCLE SUPPORT

The contractor shall participate throughout the SDLC to ensure security is an integral part of GSA business processes. The contractor shall ensure that security activities are implemented throughout the SDLC from acquisition to end of life. The ISSO shall review software releases and documentation, as assigned, to determine effects to the security posture. The contractor shall identify whether scans are required for any major, minor, patch, or data refresh releases submitted based on the documentation provided and Government policy. The contractor shall manage the configuration management and engineering change control processes (as applicable) to create security feedback loops, which help to provide the most streamlined security reviews, and to institute corrective action strategies for application release vulnerabilities prior to implementation into the production environment. Activities shall be coordinated with appropriate OCISO Security Divisions.

The contractor shall support new user request processes (i.e., verification of initial/full access); and review monthly user inactivity reports and reconcile against GSA identity systems (e.g., LDAP) as appropriate to ensure inactive accounts are removed or disabled.

2.5.7.3 SUBTASK 3 – CONTINUOUS MONITORING

The contractor shall ensure continuous monitoring of assigned information systems. The contractor shall assist in the transition from static security assessment and authorization processes and security management to continuous monitoring, and shall ensure assigned systems are compliant with continuous monitoring requirements.

The contractor shall ensure the GSA Continuous Monitoring Program is implemented for assigned systems in accordance with GSA CIO-IT Security 12-66 and as documented in the system's security plan and Continuous Monitoring Plan. The contractor shall assist the ISSM in maintaining the overall security posture of the information system by monitoring, analyzing, and reporting on automated security controls for information systems active within the OCISO Continuous Monitoring Program. The contractor shall maintain and review continuous monitoring metrics, which will assist in maintaining clear and meaningful indicators of systems' security posture.

The contractor shall monitor system security audit trails, SIEM reports, and system security documentation to ensure security measures are implemented effectively.

2.5.7.4 SUBTASK 4 – REPORTING AND DOCUMENTATION REQUIREMENTS

The contractor shall support development and maintenance of security documentation including, but not limited to, the System Security Plan, Continuous Monitoring Plan, Configuration Management Plan, Contingency Plan, Contingency Plan Test Report, POA&M, user recertification, annual FISMA assessment, and incident reports. Incidents reports are developed as necessary, POA&Ms are updated quarterly, all other documents are updated at least annually or when there is a major change as defined in GSA IT Security Procedural Guide 06-30, *Managing Enterprise Risk*.

The contractor shall ensure Privacy Impact Assessments (PIAs) are completed for IT systems that are new, under development, or undergoing major modifications which impact Privacy Act data.

The contractor shall provide support for data calls. These data calls include IT security, FISMA Assessments, IT security metrics, annual access list review, capital planning, budgeting, and capital planning, which includes developing a risk register, operations analysis, and the IT security sections of the Exhibit 300 to support the ISSM. Additionally, the contractor shall support the ISSM in the development of IT security procedural guidelines.

The contractor shall be responsible for all users who operate on its assigned system(s). As such, the contractor shall ensure compliance with HSPD-12 requirements and processes. The contractor shall verify that system users have the required authorization, background investigations, need-to-know, and access to internal security practices before access is granted to the system(s) for which the contractor has responsibility.

2.5.7.5 SUBTASK 5 – TRAINING

The contractor shall:

a. Ensure users of assigned information systems (including contractors) have completed IT Security training; IT Security Training is coordinated through the OCISO Policy and Compliance Division.

b. Promote information security awareness and provide training as assigned for IT security.
c. Comply with GSA training requirements for individuals with significant security responsibilities.

2.5.7.6 SUBTASK 6 – AUDIT SUPPORT

When there is an audit of the information system within its control, the contractor shall provide active participation as an active member of the audit team. This includes providing guidance, audit documentation review, and coordination with stakeholders. Activities cover the audit spectrum phases of pre-audit, audit, and post-audit. The contractor shall continue to remain an active key participant and team member throughout the entire process.

The contractor shall support in the investigation of theft of devices involving assigned systems; activities shall be coordinated with the OCISO SecEng division that has responsibility for incident reporting and response. The contractor may be required to participate in Office of Inspector General (OIG) investigations.

2.5.7.3 SUBTASK 7 – GOVERNANCE

The contractor shall provide information assurance subject matter expertise to GSA governance boards, assisting during the business requirements gathering phase to ensure that security controls are considered during the early stages of new initiatives. The contractor shall assist in ascertaining the best solution that also enables the business to fulfill its goal to support the end customer in the most efficient manner possible.

Contractor ISSOs shall provide a detailed approach that addresses the functional delivery of the specified tasks listed in this section for ISSO support. Tasks will be prioritized and allocated by an assigned Government ISSM.

	FY15	**FY16**	**FY17**	**FY18**	**FY19**
# of Supported information systems /Organization	3 / OCSIT 26 (22 current; 4 new) / PBS	3 / OCSIT 26 (22 current; 4 new) / PBS	3 / OCSIT 26 (22 current; 4 new) / PBS	3 / OCSIT 26 (22 current; 4 new) / PBS	3 / OCSIT 26 (22 current; 4 new) / PBS
Total # of current known systems requiring ISSOs	**29**	**29**	**29**	**29**	**29**

2.5.8 TASK 8 – REGIONAL INFORMATION SYSTEM SECURITY OFFICER SUPPORT

The contractor shall provide regional ISSO support for the Staff Offices ISSO Division. This support consists of the set of responsibilities as listed in 2.5.7 Task 7 - INFORMATION SYSTEM SECURITY OFFICER SUPPORT **plus** the responsibilities listed below:

a. Perform mobile application assessments in support of GSA IT mobile apps.
b. Monitor GSA's implementation of GSA IT implemented cloud solutions (currently Google Apps Premier, ServiceNow and Salesforce.com) for conformance to Cloud Security assessment and authorization (A&A) requirements, conduct periodic auditing, perform security training of cloud service implementations of the above cloud services and advise system custodians on potential security issues with these cloud platforms.
c. Provide IT administrative support in the area of IT business continuity to include developing and maintaining documentation on national/regional business policies and procedures related to business continuity and Continuity of Operations (COOP) for GSA IT systems.
d. Develop business processes documents for GSA IT information systems

The contractor shall primarily perform task 2.5.8 at the GSA Federal Building, 819 Taylor Street, Fort Worth, Texas 76102. Occasionally, regional travel to GSA IT regional and field sites or GSA Headquarters in Washington, D.C. for reviews, consultation, and security support may be required. The regional ISSOs will be supporting GSA IT general support systems (GSS) listed in following table. The number of current GSA IT systems and related information system security officer support requirements could increase in the future as GSA consolidates information systems under GSA IT.

	FY15	FY16	FY17	FY18	FY19
# of Supported information systems /Organization	None	5 Large GSSs GSS OCIO	5 Large GSSs GSS OCIO	5 Large GSSs OCIO	5 Large GSSs OCIO

2.5.9 TASK 9 – SECURITY ASSESSMENT AND AUTHORIZATION SUPPORT

Security authorization is the formal management decision by the Approving Official (AO) to accept the risk to operations, assets, and/or individuals based on the implementation of an agreed-upon set of security controls in order to authorize operation of an information system. By accrediting an information system, the AO is accepting responsibility for the security of the system and becomes fully accountable for any adverse impacts should a breach of security occur.

It is essential that the AO has the most complete, accurate and trustworthy information possible

on the security status of the information systems in order to make timely, credible, risk-based decisions as to whether to authorize system operations. The information and supporting evidence needed for security accreditation is developed during a detailed security review of an information system, typically referred to as security certification.

Governance of the security assessment and authorization process is currently provided by:

GSA Policy and Guidelines

a. GSA Information Technology (IT) Security Policy, CIO P 2100.1I
b. GSA Order CPO 1878.1, "GSA Privacy Act Program," dated October 27, 2003
c. GSA IT Security Procedural Guide 06-30, "Managing Enterprise Risk"
d. GSA IT Security Procedural Guide 06-29, "Contingency Plan Testing"
e. GSA IT Security Procedural Guide 09-44, "Plan of Action and Milestones (POA&M)"
f. GSA IT Security Procedural Guide 11-51, "Conducting Penetration Test Exercises"

NIST Federal Information Processing Standards (FIPS) and Guidelines

a. NIST Federal Information Processing Standard (FIPS) Publication 199
b. NIST FIPS 200
c. NIST Special Publication 800-18, Revision 1.
d. NIST Special Publication 800-34, Revision 1
e. NIST Special Publication 800-37, Revision 1
f. NIST Special Publication 800-47, Revision 1
g. NIST Special Publication 800-53, Revision 3

As security assessment and authorization governance policy and guides are updated or augmented, the contractor will be required to perform all services in accordance with the standards and policies in effect at that time.

The contractor shall provide the AO with the necessary documentation to make informed decisions regarding risk acceptance. The contractor shall provide independent security assessment for GSA information systems (to include internal Government systems, systems hosted at contractor data centers, and systems owned and operated by GSA vendors/contractors) as required by Federal and GSA governance. The contractor shall be required to provide a Security Assessment Report and a Penetration Test Report as part of authorization package. The security assessment and penetration test must be completed in accordance with GSA policy and guidelines as reflected below:

a. Security Assessment Report (with required appendices (see Appendix B of GSA IT Security Procedural Guide 06-30, "Managing Enterprise Risk")).
b. An Independent Penetration Test Report documenting the results of vulnerability analysis and exploitability of identified vulnerabilities completed in agreement with GSA IT Security Procedural Guide 11-51, "Conducting Penetration Test Exercises."

The contractor shall utilize to the greatest extent possible, existing vulnerability and code scanning data available from GSA enterprise systems, in particular ISO scan data (OS, Web,

config, DB, etc.) and ISE code scans for their independent assessment, to remove duplication. The contractor shall still need to perform such scanning activities (with exception of web app scanning) for contractor systems that ISO and ISE do not or cannot support. Vulnerability and code scanning data shall be current and reflective of all assets supporting the information system boundary or a representative subset as defined by GSA.

If the contractor is assessing a brand new system, in addition to the independent Security Assessment Report and a Penetration Test Report reflected above, the contractor may be required to create, and revise/update the following additional security assessment and authorization package documentation:

a. System Security Plan (SSP) completed in accordance with NIST Special Publication 800-18, Revision 1. The SSP shall include as appendices, required policies and procedures (as requested by GSA), Rules of Behavior, Interconnection Agreements (as applicable), GSA 800-53 R3 Control Tailoring Workbook, and Control Implementation Summary Table
b. Contingency Plan, including a disaster recovery plan
c. Contingency Plan Test Report completed in accordance with GSA IT Security Procedural Guide 06-29, "Contingency Plan Testing"
d. POA&M completed in accordance with GSA IT Security Procedural Guide 09-44, "Plan of Action and Milestones (POA&M)"
e. A Code Review Report should be submitted as part of the A&A package. See NIST 800-53 control SA-11, Enhancement 1 for additional details.

The Government estimates that the contractor shall be required to provide, at a minimum, the number of security assessments as follows:

Minimum # of GSA Security Assessment Support by Year and System Classification

Impact Level	**FY15**	**FY16**	**FY17**	**FY18**	**FY19**
FIPS 199 High	0	0	1	1	4
FIPS 199 Moderate	11	4	22	25	9
FIPS 199 Low	1	2	7	5	3
Uncategorized	0	0	1	0	0
Total Existing System Re-Certifications	**12**	**6**	**31**	**31**	**16**

Total Expected New Systems	**10**	**10**	**10**	**10**	**10**

2.5.10 TASK 10 – POLICY AND COMPLIANCE

The Policy and Compliance Division provides management and maintenance of the GSA security authorization, POA&M, Continuous Monitoring, Privacy, and Security Training programs. Further, the division develops and maintains GSA security, privacy, and continuous monitoring policies and procedural guidelines and supports FedRAMP as well as security audit coordination efforts.

2.5.10.1 SUBTASK 1 – PROCEDURAL GUIDELINE DEVELOPMENT AND COMPLIANCE

The contractor shall support the update of up to ten GSA IT Security Procedural Guidelines and two IT/Privacy Policies annually to align with NIST 800-53 R4 and operation of the new consolidated OCISO. This involves modifying existing guidelines/policies to be provided by the OCISO Policy and Compliance Division.

Guides requiring update are identified below:

a. Securing Mobile Devices and Applications (CIO-IT Security-12-67): The purpose of this publication is to outline how GSA centrally manages and secures mobile devices, such as smart phones and tablets, and the applications loaded on them. This publication also explains the security concerns inherent in mobile device use and provides direction on securing mobile devices throughout their life cycle.
b. Continuous Monitoring Program (CIO-IT Security-12-66): This guide defines the GSA Continuous Monitoring Program. GSA contractors and Federal employees should use this guide and the noted references when performing continuous monitoring of information systems that qualify for the GSA Configuration Management (CM) process.
c. Physical and Environmental Protection (CIO-IT Security-12-64): This guide provides guidance for a secure environment for information systems, including physical access control, fire protection, emergency power and alternate sites.
d. GSA's System and Information Integrity (CIO-IT Security-12-63): This guide provides information to assist the GSA IT security community in establishing the required federal and agency controls to meet the objectives of system integrity. System integrity is defined as the quality that a system has when it performs its intended function in an unimpaired manner, free from unauthorized manipulation of the system, whether intentional or accidental.
e. GSA's Security Implementation of the Salesforce Platform (CIO-IT Security-11-62): This guide provides GSA employees and contract personnel that have IT security responsibilities with information to implement a standard Salesforce A&A. The guide outlines the key activities for implementing the A&A process.
f. Maintenance Guide (CIO-IT-Security 10-50): This Guide provides GSA associates and contractors with a discussion of the significant security responsibilities involved in system maintenance and the specific procedures on maintaining the functional state of system hardware in order to ensure continuous and uninterrupted operation, while also

maintaining the established security configuration for the information system.

g. Security Language for IT Acquisition Efforts (CIO-IT Security 09-48): This guide establishes security language for GSA IT acquisition contracts involving contractor owned and operated systems on behalf of GSA or the Federal Government (when GSA is the managing agency).
h. Key Management (CIO IT Security 09-43): This guide provides a framework to document operating procedures and processes that are required by GSA IT Security Policies, FISMA and FIPS 140-2.
i. FISMA Implementation (CIO-IT-Security-04-26 Revision 5): FISMA Implementation defines GSA's annual FISMA Security Program Review in agreement with OMB FISMA reporting guidance, currently OMB Memorandum M-08-21, FY 2008 Reporting Instructions for the FISMA and Agency Privacy Management, dated July 14, 2008.
j. Web Server Log Review Guide (CIO IT Security 08-41): This guide is designed to give an overview of how to conduct periodic web server log review that is integral to web system operation and security oversight. It does not address the specific needs of enterprise-wide log analysis systems that aggregate logs from many servers. The guide discusses summary and detailed views of log contents.
k. Home User's Guide (CIO IT Security 04-24): The purpose of this "Home User's Guide" is two-fold: 1) to provide GSA associates and authorized individuals, to include Federal employees and contractors, with information necessary to protect home computers from possible threats and/or breaches, and 2) to ensure home computers used to connect to the GSA network have sufficient security safeguards so as to minimize threats to the GSA network.
l. Identification and Authentication (IA) (CIO IT Security 01-01): The guide provides GSA associates and contractors with significant security responsibilities as identified in the GSA IT Security Policy CIO P 2100.1 and other IT personnel involved in implementing identification and authentication, the specific processes and procedures to follow for implementing identification and authentication for the systems under their purview.
m. Configuration Management (CM) Guide (CIO IT Security 01-05): This document provides guidance for all individuals with responsibility for CM processes used by GSA.
n. GSA Contingency Plan (CP) (CIO-IT-Security 06-29): Contingency Planning provides guidance to GSA personnel involved in implementing contingency planning with specific processes and procedures to follow for the systems under their purview.
o. Access Control (CIO IT Security 01-07): This document provides guidance for individuals with responsibility for implementing appropriate access controls for GSA IT resources. Access control methods and documented procedures provide an effective and standardized process for granting or denying access for a specified user or groups of users.
p. Auditing & Monitoring (CIO IT Security 01-08): The policy provides IT personnel involved in implementing auditing and monitoring with the specific procedures to follow for implementing the function for the systems under their purview.
q. Termination Transfer Guide (CIO IT Security 03-23): This guide provides for the establishment and implementation of the IT Security notification procedures for terminated or transferred GSA associates and contractors with access to GSA IT resources and data. The purpose of these procedures is to improve access security controls over all GSA IT resources.

r. Managing Enterprise Risk: Security Assessment and Authorization, Planning and Risk Assessment (CA, PL &RA) (CIO IT Security 06-30): This guide describes the key activities in managing enterprise-level risk, as described in NIST 800-37 and the NIST Enterprise Risk Framework. GSA contractors and Federal associates should use this guide and the noted reference for performing A&A activities.
s. Media Protection Guide (CIO IT Security 06-32): This guide defines media protection requirements as identified in GSA Order CIO P 2100, GSA Information Technology (IT) Security Policy and NIST SP 800-53.
t. IT Security Procedural Guide: IT Security Training and Awareness Program (CIO Security 05-29) - IT Security Awareness Program and GSA Order.
u. Privacy Act Program (1878.1 CPO): Establishes the Privacy Act Program website as the official vehicle for disseminating program policy and procedures.
v. Conducting Privacy Impact Assessments (PIAs) in GSA (1878.2B) CPO: Policy and procedures for addressing privacy issues in GSA IT systems, online websites, and social media venues containing Personally Identifiable Information (PII) about individuals.
w. Rules of Behavior for Handling Personally Identifiable Information (PII) (2180.1 HCO): Policy on how to properly handle PII and the consequences and corrective actions that will be taken when a breach has occurred.
x. Data Release Policy (9297.1 HCO): Policy on releasing information relating to GSA employees, contractors, and others for whom GSA maintains information.
y. Information Breach Notification Policy (9297.2B HCO): Policy on what actions should be taken when it is determined that PII has been compromised and employees and contractors need to be notified.
z. Continuous Monitoring and Ongoing Authorizations (CIO IL-12-02): The purpose of this Instructional Letter (IL) is to provide direction and guidance for information systems with new, existing and expiring authorizations (Authority-to-Operate (ATO)) to transition to a Continuous Monitoring Program and ongoing authorizations.

Additional procedural guides may be required as necessary. Also, identified guides may be replaced by different guides as necessary.

2.5.10.2 SUBTASK 2 – SECURITY AUTHORIZATION PACKAGES, PLAN OF ACTION AND MILESTONES, AND SYSTEM CONTINUOUS MONITORING PLANS

The contractor shall perform compliance reviews of system security authorization packages for internal GSA IT systems as well as for FedRAMP packages of cloud service providers, POA&M, and Continuous Monitoring Plans.

The FedRAMP program provides Cloud Service Providers (CSPs) an opportunity to obtain a Provisional Authorization to operate from the Joint Authorization Board (JAB) after undergoing a third-party independent security assessment.

Security Authorization Package Compliance Reviews

Security Authorization package compliance reviews ensure that the Authorizing Official is presented with complete and reliable security authorization packages to facilitate an informed system ATO decision based on risks and controls implemented.

The guidelines for GSA security authorization packages are documented in Managing Enterprise

Risk: Security Assessment and Authorization, Planning and Risk Assessment (CA, PL & RA) (CIO IT Security 06-30). The guidelines for FedRAMP security authorization packages are documented on the FedRAMP site available at http://www.gsa.gov/portal/category/102371.

The contractor shall review GSA and FedRAMP cloud service provider security assessment packages to ensure compliance with documented GSA and FedRAMP processes and requirements, respectively. The contractor shall review documentation and findings in security authorization packages for adherence to GSA and FedRAMP quality and acceptability criteria.

OCISO anticipates upwards of 40 GSA security authorization packages and 20 FedRAMP security authorization package reviews annually.

Plan of Action and Milestones (POA&M) Compliance Reviews

The contractor shall perform compliance reviews of system Plan of Action and Milestones POA&M to ensure system POA&Ms are completed in accordance with GSA IT Security Procedural Guide 09-44, Plan of Action and Milestones. OCISO anticipates 120 system POA&Ms to be reviewed quarterly.

Continuous Monitoring Plan Compliance Reviews

Continuous Monitoring, as described in guide GSA IT Security Procedural Guide, 12-66, ensures that the Government uses a more dynamic, outcome-focused approach to continuous monitoring that facilitates ongoing authorizations. OCISO anticipates ten Continuous Monitoring Plans to be reviewed annually.

This page intentionally left blank.

4.1 PLACE OF INSPECTION AND ACCEPTANCE

Inspection and acceptance of all work performance, reports, and other deliverables under this TO shall be performed by the FEDSIM COR at GSA Headquarters.

4.2 SCOPE OF INSPECTION

All deliverables will be inspected for content, completeness, accuracy, and conformance to TO requirements by the FEDSIM COR. Inspection may include validation of information or software through the use of automated tools, testing, or inspections of the deliverables, as specified in the TO. The scope and nature of this inspection will be sufficiently comprehensive to ensure the completeness, quality, and adequacy of all deliverables.

The Government requires a period NTE 15 workdays after receipt of final deliverable items for inspection and acceptance or rejection by the COR.

4.3 BASIS OF ACCEPTANCE

The basis for acceptance shall be compliance with the requirements set forth in the TO, the contractor's quote, and relevant terms and conditions of the contract. Deliverable items rejected shall be corrected in accordance with the applicable clauses.

Reports, documents, and narrative-type deliverables will be accepted when all discrepancies, errors, or other deficiencies identified in writing by the Government have been corrected.

If the draft deliverable is adequate, the Government may accept the draft and provide comments for incorporation into the final version.

All of the Government's comments on deliverables must either be incorporated in the succeeding version of the deliverable, or the contractor must demonstrate to the Government's satisfaction why such comments should not be incorporated.

If the Government finds that a draft or final deliverable contains spelling errors, grammatical errors, or improper format, or otherwise does not conform to the requirements stated within this TO, the document may be immediately rejected without further review and returned to the contractor for correction and resubmission. If the contractor requires additional Government guidance to produce an acceptable draft, the contractor shall arrange a meeting with the FEDSIM COR.

4.4 DRAFT DELIVERABLES

The Government will provide written acceptance, comments, and/or change requests, if any, within 15 workdays (unless specified otherwise in Section 5 - Deliverables or Performance) from Government receipt of the draft deliverable.

Upon receipt of the Government comments, the contractor shall have ten workdays to incorporate the Government's comments and/or change requests and to resubmit the deliverable in its final form.

4.5 WRITTEN ACCEPTANCE/REJECTION BY THE GOVERNMENT

The CO/COR will provide written notification of acceptance or rejection (Section 9 – List of Attachments, Attachment I) of all final deliverables within 15 workdays (unless specified otherwise in Section 5 - Deliverables or Performance). All notifications of rejection will be accompanied with an explanation of the specific deficiencies causing the rejection.

5.1 PERIOD OF PERFORMANCE

The period of performance for this TO is a one-year base period and four, one-year options.

5.2 PLACE OF PERFORMANCE

Place of performance will primarily be at GSA Headquarters at 1800 F street NW, Washington DC. Section 2.5.8, Task 8 Regional Information System Security Officer Support, shall be performed at 819 Taylor Street, Fort Worth, TX with occasional travel to regional offices. All contractors, regardless of locale, are expected to work from the designated GSA offices and may be allowed to telework from either the contractor's office or home office at the Government's discretion (typically 2-3 days a week).

5.3 TASK ORDER SCHEDULE AND MILESTONE DATES

The following schedule of milestones will be used by the FEDSIM COR to monitor timely progress under this TO.

The following abbreviations are used in this schedule:

NLT: No Later Than
TOA: Task Order Award
All references to Days: Government Workdays

Deliverables are due the next Government workday if the due date falls on a holiday or weekend.

The contractor shall deliver the deliverables listed in the following table:

MILESTONE/DELIVERABLE	SOW REFERENCE	PLANNED COMPLETION DATE
Project Start (PS)		At TOA
Kick-Off Meeting	2.5.1.1	Within 5 workdays of TOA
Transition in Plan	2.5.1.1	Due at Kick-Off Meeting
Monthly Status Report	2.5.1.2	Monthly; within the 10th calendar day of the next month
Draft Project Management Plan	2.5.1.3	Due at Kick-Off Meeting and updates at least semi-annually
Project Management Plan – Comments	2.5.1.3	5 workdays after Government receipt
Project Management Plan – Final	2.5.1.3	10 workdays after receipt of Government comments
Integrated Master Schedule -Draft	2.5.1.3	Due at Kick-Off Meeting
Integrated Master Schedule - Comments	2.5.1.3	10 workdays after Government receipt

MILESTONE/DELIVERABLE	SOW REFERENCE	PLANNED COMPLETION DATE
Integrated Master Schedule (IMS) – Final	2.5.1.3	NLT 20 workdays after receipt of Government Comments then monthly thereafter
Transition-In and Transition-Out Plan – Drafts	2.5.2	Due at Kick-Off Meeting. Transition-Out Plan Updatesl due 10 workdays after the exercise of each option period.
Transition-In Plan – Comments	2.5.2	5 workdays after Government receipt
Transition-In Plan – Final	2.5.2	10 workdays after receipt of Government comments
Transition-Out Plan – Comments	2.5.2	5 workdays after Government receipt
Transition-In Plan – Final	2.5.2	10 workdays after receipt of Government comments
Quarterly Wireless Scanning and Vulnerability Reports	2.5.4.1	In accordance with IMS
War Dialing Penetration Testing	2.5.4.2	In accordance with IMS
Vulnerability and Configuration Scanning	2.5.4.3	Weekly in accordance with IMS
Vulnerability Scanning (Web Applications)	2.5.4.4	Scans monthly in accordance with IMS
Vulnerability and Configuration Scanning (Database)	2.5.4.5	Monthly Scans in accordance with IMS
Develop and Maintain Hardening Guides	2.5.5.1	In accordance with IMS
Desktop Software Testing and Documentation	2.5.5.2	In accordance with IMS
Update and Maintain incident management process documents	2.5.5.4	Every 6 months and after Major IT security Incidents as determined by the Government
Manual Penetration Test plan	2.5.5.5	To be submitted to Government 3 days prior to Penetration Testing
Manual Penetration Testing	2.5.5.5	In accordance with IMS
Software Code Review and Documentation	2.5.5.6	In accordance with IMS

MILESTONE/DELIVERABLE	SOW REFERENCE	PLANNED COMPLETION DATE
Update Software Code Review Process Documents	2.5.5.6	Bi-Annually in accordance with IMS or after major changes in policy
Software Code Review Training Sessions	2.5.5.6	4 times per year in accordance with IMS
SEIM and SOC Monitoring and Analysis	2.5.6.1	Within 4 business hours of incident occurrence
Application Whitelisting process	2.5.6.2	In accordance with IMS
ISSO Security Documentation	2.5.7	In accordance with IMS
ISSO POA&M Updates	2.5.7	Updated at least Quarterly in accordance with IMS
Assessment and Authorization documentation including Security Assessment, and Penetration Test Reports as part of authorization packages	2.5.9	In accordance with the IMS
Updates to 10 Security Procedural Guidelines and 2 IT/Privacy Policies	2.5.10	In accordance with IMS
Security Authorization Packages	2.5.10.2	At least 40 annually in accordance with IMS
FedRAMP Security Authorization Reviews	2.5.10.2	At least 20 annually in accordance with IMS
Continuous Monitoring Plan Compliance Review	2.5.10.2	At least 10 annually in accordance with IMS
Copy of TO (initial award and all modifications)	5.3.1	Within 10 workdays of award
IT Security Plan	5.3.2	NLT 30 calendar days after TOA and annual verification or update.
IT Security Authorization	5.3.2	6 months after TOA
Trip Report(s)	6.3.4	Within 10 workdays following completion of each trip
Section 508 Product Accessibility Report	7.5	NLT 20 workdays after TOA and upon system changes affecting the report

5.3.1 PUBLIC RELEASE OF CONTRACT DOCUMENTS REQUIREMENT

The contractor agrees to submit, within ten workdays from the date of the CO's execution of the initial TO, or any modification to the TO (exclusive of Saturdays, Sundays, and Federal holidays), a portable document format (PDF) file of the fully executed document with all

proposed necessary redactions, including redactions of any trade secrets or any commercial or financial information that it believes to be privileged or confidential business information, for the purpose of public disclosure at the sole discretion of GSA. The contractor agrees to provide a detailed written statement specifying the basis for each of its proposed redactions, including the applicable exemption under the Freedom of Information Act (FOIA), 5 U.S.C. § 552, and, in the case of FOIA Exemption 4, 5 U.S.C. § 552(b)(4), shall demonstrate why the information is considered to be a trade secret or commercial or financial information that is privileged or confidential. Information provided by the contractor in response to the contract requirement may itself be subject to disclosure under the FOIA. Submission of the proposed redactions constitutes concurrence of release under FOIA.

GSA will carefully consider all of the contractor's proposed redactions and associated grounds for nondisclosure prior to making a final determination as to what information in such executed documents may be properly withheld.

5.3.2 GSA INFORMATION TECHNOLOGY (IT) SECURITY REQUIRMENTS

The contractor shall deliver an IT Security Plan within 30 calendar days of award that describes the processes and procedures that will be followed to ensure appropriate security of IT resources that are developed, processed, or used under this Order. The IT Security Plan shall comply with applicable Federal laws including, but not limited to, 40 U.S.C. 11331, the FISMA of 2002, and the E-Government Act of 2002. The IT Security Plan shall meet IT security requirements in accordance with Federal and GSA policies and procedures, including GSAR clause 552.239-71. The contractor shall submit written proof of IT security authorization six months after award, and verify that the IT Security Plan remains valid annually.

5.3.3 DELIVERABLES MEDIA

The contractor shall deliver all electronic versions by email and removable electronic media, as well as placing in the OCISO's designated repository. The following are the required electronic formats, whose versions must be compatible with the latest, commonly available version on the market.

- Text MS Word
- Spreadsheets MS Excel
- Briefings MS PowerPoint
- Drawings MS Visio
- Schedules MS Project

5.4 PLACE(S) OF DELIVERY

Unclassified deliverables or correspondence shall be delivered to the FEDSIM CO or COR at the following address:

GSA FAS AAS FEDSIM
ATTN: Carl Jablonski COR
1800 F Street NW
Suite 3100 (QF0B)
Washington, D.C. 20405
Telephone: (202) 760-5320

Email: carl.jablonski@gsa.gov

Copies of all deliverables shall also be delivered to the GSA CISO TPOC at the following address:

Contact information to be supplied after award

5.5 NOTICE REGARDING LATE DELIVERY/ PROBLEM NOTIFICATION REPORT (PNR)

The contractor shall notify the FEDSIM COR via a Problem Notification Report (PNR) (Section 9 - List of Attachments, Attachment G) as soon as it becomes apparent to the contractor that a scheduled delivery will be late. The contractor shall include in the PNR the rationale for late delivery, the expected date for the delivery, and the project impact of the late delivery. The FEDSIM COR will review the new schedule and provide guidance to the contractor. Such notification in no way limits any Government contractual rights or remedies including, but not limited to, termination.

6.1 CONTRACTING OFFICER'S REPRESENTATIVE (COR)

The CO will appoint a COR in writing for each TO through a COR Appointment Letter that will be provided to the contractor upon award (Section 9, - List of Attachments, Attachment A). The COR will receive, for the Government, all work called for by the TO and will represent the CO in the technical phases of the work. The COR will provide no supervisory or instructional assistance to contractor personnel.

The COR is not authorized to change any of the terms and conditions, scope, schedule, and price of the Contract or the TO. Changes in the scope of work will be made only by the CO by properly executed modifications to the Contract or the TO.

6.1.1 CONTRACT ADMINISTRATION

Contracting Officer:

John Terrell
GSA FAS AAS FEDSIM
1800 F Street NW
Suite 3100 (QF0B)
Washington, DC 20405
Telephone: (703) 605-2748
Email: john.terrell@gsa.gov

Contracting Officer's Representative:

Carl Jablonski
GSA FAS AAS FEDSIM
1800 F Street NW
Suite 3100 (QF0B)
Washington, D.C. 20405
Telephone: (202) 760-5320
Email: carl.jablonski@gsa.gov

Technical Point of Contact:

Provided after award.

6.2 INVOICE SUBMISSION

The contractor shall submit Requests for Payments in accordance with the format contained in General Services Administration Acquisition Manual (GSAM) 552.232-25, PROMPT PAYMENT (NOV 2009), to be considered proper for payment. In addition, the following data elements shall be included on each invoice.

Task Order Number: *(from GSA Form 300, Block 2)*
Paying Number: *(ACT/DAC NO.) (From GSA Form 300, Block 4)*
FEDSIM Project Number: GS00658
Project Title: Security Engineering and Operations Support

The contractor shall certify with a signed and dated statement that the invoice is correct and proper for payment.

The contractor shall provide invoice backup data in accordance with the contract type, including detail such as labor categories, rates, and quantities of labor hours per labor category.

The contractor shall submit invoices as follows:

The contractor shall utilize FEDSIM's electronic Tracking and Ordering System (TOS) to submit invoices. The contractor shall submit invoices electronically by logging onto the following link (requires Internet Explorer to access the link):

https://portal.fas.gsa.gov

Select *Vendor Support,* log in using your assigned I.D. and password, then click on *Create Invoice*. The TOS Help Desk should be contacted for support at 877-472-4877 (toll free). By utilizing this method, no paper copy of the invoice shall be submitted to GSA FEDSIM or the GSA Finance Center. However, the FEDSIM COR may require the contractor to submit a written "hardcopy" invoice with the client's certification prior to invoice payment.

6.3 INVOICE REQUIREMENTS

The contractor shall submit simultaneous copies of the invoice to both GSA and the client POC. Receipts are provided on an as requested basis.

If the TO has different contract types, each should be addressed separately in the invoice submission.

The final invoice is desired to be submitted within six months of project completion.

6.3.1 TIME-AND-MATERIAL (T&M) CLINs (for LABOR)

The contractor may invoice monthly on the basis of cost incurred for the T&M CLINs. The invoice shall include the period of performance covered by the invoice and the CLIN number and title. All hours and costs shall be reported by CLIN element (as shown in Section 1 – Supplies or Services and Price/Costs), by contractor employee, and shall be provided for the current billing month and in total from project inception to date. The contractor shall provide the invoice data in spreadsheet form with the following detailed information. The listing shall include separate columns and totals for the current invoice period and the project to date.

a. Employee name (current and past employees)
b. Employee company labor category (from IT 70 contract)
c. Employee labor category
d. Monthly and total cumulative hours worked
e. Corresponding ceiling rate
f. Cost incurred not billed

6.3.2 FIRM-FIXED-PRICE (FFP) CLINs

The contractor may invoice as stated in Section 1 – Supplies or Services and Price/Costs for the FFP CLINs. The invoice shall include the period of performance covered by the invoice and the CLIN number and title. All costs shall be reported by CLIN element (as shown in Section 1 –

Supplies or Services and Price/Costs) and shall be provided for the current invoice and in total from project inception to date. The contractor shall provide the invoice data in spreadsheet form with the following detailed information. The listing shall include separate columns and totals for the current invoice period and the project to date.

6.3.3 OTHER DIRECT COSTS (ODCs)

The contractor may invoice monthly on the basis of cost incurred for the ODC CLINs. The invoice shall include the period of performance covered by the invoice and the CLIN number and title and Interagency Agreement (IA) number. In addition, the contractor shall provide the following detailed information for each invoice submitted, as applicable. Spreadsheet submissions, in MS Excel format, are required.

a. ODCs purchased
b. Date delivery accepted by the Government
c. Associated CLIN
d. Project-to-date totals by CLIN
e. Cost incurred not billed
f. Remaining balance of each CLIN
g. Indirect Handling Rate

6.3.4 TRAVEL

The contractor may invoice monthly on the basis of cost incurred for cost of travel comparable with the Federal Travel Regulation (FTR). The invoice shall include the period of performance covered by the invoice, the CLIN number and title, and the IA number. Separate worksheets, in MS Excel format, shall be submitted for travel.

CLIN/Task Total Travel: This invoice information shall identify all cumulative travel costs billed by CLIN/Task. The current invoice period's travel details shall include separate columns and totals and include the following:

a. Travel Authorization Request identifier, approver name, and approval date
b. Current invoice period
c. Names of persons traveling
d. Number of travel days
e. Dates of travel
f. Number of days per diem charged
g. Per diem rate used
h. Total per diem charged
i. Transportation costs (rental car, air fare, etc.)
j. Total charges
k. Explanation of variances exceeding 10% of the approved versus actual costs
l. Indirect handling rate

7.1 ON-SITE AND OFFSITE RATES

If the Contractor's GSA Schedule contains on-site and off-site rates, those rates shall apply, as appropriate. In the event that the underlying GSA Schedule does not identify the labor rate for employee performance when performance occurs outside of a Contractor facility (e.g., teleworking from home), on-site rates shall apply.

7.2 KEY PERSONNEL

The following are the minimum personnel who shall be designated as "Key." The Government does not intend to dictate the composition of the ideal team to perform this TO. Therefore, the Government encourages and will evaluate additional Key Personnel as proposed by the offeror. Should additional Key Personnel be proposed, the Government will apply the same requirements and evaluation criteria to these as are applied to the required Key Personnel.

a. Program Manager (PM)
b. Security Engineering Specialist
c. Security Operations Specialist
d. Assessment and Authorization Compliance Specialist

The Government desires that Key Personnel be assigned for the duration of the TO. Key Personnel may be replaced or removed subject to Section 7.1.5 - Special Contract Requirements, Key Personnel Substitution.

7.2.1 PROGRAM MANAGER

The contractor shall provide a PM who is responsible for the day-to-day oversight of contractor personnel and TO performance. The PM shall have full authority to make all commitments and decisions for all elements of the TO. The PM should proactively address all Government concerns to the best of their ability.

It is required that the PM has the following qualifications:

- PM possesses a project management certification, such as Project Management Institute (PMI) Project Management Professional (PMP).

It is desirable that the PM has the following qualifications:

- Experience with designing and implementing information security plans for enterprises with diverse sets of complex applications, databases, network connections, and communications subsystems.
- Experience with implementing security procedures in accordance with best practice methodologies such as Carnegie Mellon's Software Engineering Institute (SEI) CMMI standards, and/or the IT Information Library (ITIL).
- Knowledge of Federal IT policy, regulations, and best practices to include NIST and FIPS guidelines.

7.2.2 SECURITY ENGINEERING SPECIALIST

The contractor shall provide a Security Engineering Specialist. This specialist shall be responsible for ensuring the quality of all performance under tasks relating to security engineering. The Security Engineering Specialist shall be responsible for all activity related to software testing, incident response and management, forensic analysis and other emerging enterprise-wide IT challenges.

It is desired that the Security Engineering Specialist has the following qualifications:

- BS or greater in Computer Engineering, Electrical Engineering, or Systems Engineering
- Possess at least ten years of specialized experience in incident response, management of the APT, forensic analysis, testing and software code review, and handling of evidentiary data with the most recent experience in the past three years.
- Extensive Knowledge of web application security, secure coding and source code reviews (Python, Java, C, C++, .NET, APEX, RoR, etc,) cloud security, virtualization security, Building/Physical Security, and MS Network architecture and design.
- Possess in depth knowledge of Windows, Linux and Unix/Solaris operating systems with at least five years of experience developing hardening benchmarks and creating, testing, and utilizing SCAP content.

7.2.3 SECURITY OPERATIONS SPECIALIST

The contractor shall provide a Security Operations Specialist. This Security Operation Specialist shall be responsible for all performance under tasks relating to security operations (Sections 2.5.4 and 2.5.6).

It is required that the Security Operations Specialist has the following qualifications:

- Security Operations Specialist possesses the CISSP designation.

It is desirable that the Security Operations Specialist have the following qualifications:

- Expert knowledge of Federal IT security standards (i.e., FISMA) and auditing standards.
- Possess at least five years of experience with enterprise OS scanning, configuration scanning, database scanning, and web application scanning and testing in environments of similar size and scope, with hands-on experience in the past three years.
- Expert knowledge of penetration testing tools, application white listing tool management, server and database management, and command line scripting, with hands-on experience in the past three years.
- Experience within the last three years managing SQL servers and testing/running queries against Oracle servers.
- At least 5 years of experience with triaging vulnerabilities, writing and executing hardening guides, creating or modifying and implementing SCAP content, penetration testing, wifi-scanning and war dialing.
- Possess in depth knowledge of Windows, Linux and Unix/Solaris operating systems and network and wireless protocols.

7.2.4 ASSESSMENT AND AUTHORIZATION (A&A), ISSO, FEDRAMP SPECIALIST

The contractor shall provide an A&A Compliance Specialist for this TO. The contractor shall be responsible for ensuring all A&As are done completely, without error, and in compliance with all applicable rules and regulations.

It is required that the A&A Compliance Specialist has the following qualifications:

- Current CISSP designation.
- At least five years of experience developing the required documents for the A&A package (e.g., SSP, CP, and SAR), including oversight and development of POA&M's, and performing all continuous monitoring functions with the most recent experience occurring in the last three years.

It is desired that the A&A Compliance Specialist has the following qualifications:

- At least five years of experience with and detailed knowledge of FedRAMP, NIST, OMB, US-CERT, and CISSP with the most recent experience in the last three years
- Experience in applying risk management techniques to develop and complete risk assessments based on NIST standards to ensure system design and implementation sufficiently addresses or mitigates IA risk.
- At least five years of experience implementing NIST 800-53a security controls for Federal agencies

7.2.5 KEY PERSONNEL SUBSTITUTION

The contractor shall not replace any personnel designated as Key Personnel without the written concurrence of the CO. Prior to utilizing other than personnel specified in proposals in response to a RFQ, the contractor shall notify the Government CO and the COR of the existing TO. This notification shall be no later than 15 calendar days in advance of any proposed substitution and shall include justification (including resume(s) and labor category of proposed substitution(s)) in sufficient detail to permit evaluation of the impact on TO performance.

Substitute personnel qualifications shall be equal to, or greater than, those of the personnel being substituted. If the Government CO and the COR determine that a proposed substitute personnel is unacceptable, or that the reduction of effort would be so substantial as to impair the successful performance of the work under the TO, the contractor may be subject to default action as prescribed by FAR 52.249-6 Termination (Cost Reimbursement) or FAR 52.249-8, Default (Fixed-Price Supply and Service).

7.3 GOVERNMENT-FURNISHED PROPERTY (GFP)

The GFP is listed in Section 9 - List of Attachments, Attachment F). The GFP will be provided during transition in and as required by the tasks in the SOW.

7.4 SECURITY REQUIREMENTS

The contractor shall be responsible for properly protecting all information used, gathered, or developed as a result of this TO. The contractor shall implement procedures to ensure that

appropriate administrative, technical, and physical safeguards are established to ensure the security and confidentiality of sensitive Government information, data, and/or equipment. The contractor's procedures shall be consistent with Government and GSA policies, including GSA Order 2100.3A, Information Technology Security Policy (or most current version), OMB Memorandums & Circulars, FISMA, the Computer Security Act of 1987, and the Privacy Act. In addition, during all activities and operations on Government premises, the contractor shall comply with the policies, rules, procedures and regulations governing the conduct of personnel or protection of Government facilities and data as expressed by GSA, written or oral.

7.4.1 PROTECTION OF INFORMATION

The contractor shall be responsible for properly protecting all information used, gathered, or developed as a result of work under this TO. The contractor shall also protect all Government data, and equipment by treating the information as sensitive. All information about the systems gathered or created under this TO should be considered as sensitive but unclassified information. It is anticipated that this information will be gathered, created and stored within the primary work location. If contractor personnel must remove any information from the primary work area they shall protect it to the same extent they would their proprietary data and/or company trade secrets. The use of any information that is subject to the Privacy Act will be utilized in full accordance with all rules of conduct as applicable to Privacy Act Information.

7.4.2 SECURITY CONSIDERATIONS

The contractor shall comply with agency personal identity verification procedures identified in the RFQ that implement HSPD 12 Information Processing Standards Publication (FIPS PUB) Number 201. The contractor shall insert this clause in all subcontracts when the subcontractor is required to have physical access to a Federally controlled facility or access to a Federal Information System. Work on this project may require contractor personnel to have access to limited information to fully integrate financial, operational, procurement, and personnel data. The clearance is considered sensitive, but unclassified. All contractors issued a GSA email address shall maintain current contact information in the GSA Credential and Identity Management System (GCIMS) system.

Contractors shall comply with GSA Order 2100.1 - "IT Security Policy," GSA Order ADM 9732.1C - "Suitability and Personnel Security," and OCHCO/OCIO HSPD-12 Personal Identity Verification and Credentialing Standard Operating Procedures (SOP). Background investigations are required for access to GSA information systems (including contractor operations that design, operate, test, maintain, and/or monitor GSA systems). The applications in scope of this TO are categorized as "Moderate Risk" systems; therefore, contractors supporting the project shall be required to undergo a Minimum Background Investigation (MBI). The contractor shall adhere to all security-related laws, requirements, and regulations that bind the Government. The contractor shall have all staff members complete a confidentiality agreement prior to working under this contract. Contractor personnel involved in the management, operation, programming, maintenance, and/or use of IT shall be aware of these responsibilities and fulfill them. Detailed security responsibilities for the contractor are found in the GSA Orders/Handbooks listed in the RFQ.

Contractor personnel working under this TO will not be required to have a security clearance. When Government on-site meetings are required, the Government will provide personnel to ensure approved contractor personnel have access to Government facilities. Selected contractor employees may be required to complete mandatory Security Awareness and Privacy Training (this training is often provided internally by GSA via GSA Online University).

The contractor shall be responsible for properly protecting all information used, gathered, or developed as a result of the TO. The contractor shall implement procedures to ensure that appropriate administrative, technical, and physical safeguards are established to ensure the security and confidentiality of sensitive Government information, data, and/ or equipment. The contractor's procedures shall be consistent with Government and GSA policies, including GSA Order 2100.1, Information Technology Security Policy (or most current version), OMB Memorandums & Circulars, FISMA, the Computer Security Act of 1987, and the Privacy Act. In addition, during all activities and operations on Government premises the contractor shall comply with the policies, rules, procedures and regulations governing the conduct of personnel or protection of Government facilities and data as expressed by GSA, written or oral.
The contractor shall be responsible for properly protecting all information used, gathered, or developed as a result of work under this TO. The contractor shall also protect all Government data and equipment by treating the information as sensitive. The use of any information that is subject to the Privacy Act will be utilized in full accordance with all rules of conduct as applicable to Privacy Act Information.

7.5 ORGANIZATIONAL CONFLICT OF INTEREST AND NON-DISCLOSURE REQUIREMENTS

7.5.1 ORGANIZATIONAL CONFLICT OF INTEREST

If the contractor or proposed subcontractors or GSA Schedule Contractor Team Arrangement (CTA) members has provided, is currently providing, or anticipates providing support to GSA involving GSA IT security and privacy program services, the offeror shall immediately disclose this fact to the Contracting Officer in accordance with FAR Subpart 9.5. Work on any of these must be disclosed regardless of whether the offeror is or was the prime contractor, subcontractor, CTA member or consultant on the effort. The contractor is also required to complete and sign an Organizational Conflict of Interest Statement in which the contractor (and any subcontractors, consultants or CTA members) agrees to disclose information concerning the actual or potential conflict with any quote for any solicitation relating to any work in the TO. All actual or potential OCI situations shall be handled in accordance with FAR Subpart 9.5 and may require the offeror to submit a mitigation plan.

7.5.2 NON-DISCLOSURE REQUIREMENTS

If the contractor acts on behalf of, or provides advice with respect to any phase of an agency procurement, as defined in FAR 3.104-4, then the contractor shall ensure that all its personnel (to include subcontractors, CTA members, and consultants) who will be personally and substantially involved in the performance of the TO:

a. Execute and submit an Corporate Non-Disclosure Agreement (NDA) Form (Section 9 - List of Attachments, Attachment D) prior to the commencement of any work on the TO, and
b. Are instructed in the FAR 3.104 requirements for disclosure, protection, and marking of contractor bid or quote information, or source selection information.

All proposed replacement contractor personnel also must submit a Non-Disclosure Agreement and be instructed in the requirements of FAR 3.104. Any information provided by contractors in the performance of this TO or obtained by the Government is only to be used in the performance of the TO. The contractor shall put in place appropriate procedures for the protection of such information and shall be liable to the Government for any misuse or unauthorized disclosure of such information by its personnel, as defined above.

7.6 SECTION 508 COMPLIANCE REQUIREMENTS

Unless the Government invokes an exemption, all Electronic and Information Technology (EIT) products and services proposed shall fully comply with Section 508 of the Rehabilitation Act of 1973, per the 1998 Amendments, 29 United States Code (U.S.C.) 794d, and the Architectural and Transportation Barriers Compliance Board's Electronic and Information Technology Accessibility Standards at 36 Code of Federal Regulations (CFR) 1194. The contractor shall identify all EIT products and services proposed, identify the technical standards applicable to all products and services proposed, and state the degree of compliance with the applicable standards. Additionally, the contractor must clearly indicate where the information pertaining to Section 508 compliance can be found (e.g., Vendor's or other exact web page location). The contractor must ensure that the list is easily accessible by typical users beginning at time of award.

7.7 TRAVEL

7.7.1 TRAVEL REGULATIONS

Contractor costs for travel will be reimbursed at the limits set in the following regulations (see FAR 31.205-46):

a. Federal Travel Regulations (FTR) - prescribed by the GSA, for travel in the contiguous United States (U.S.)

7.7.2 TRAVEL AUTHORIZATION REQUESTS

Before undertaking travel to any Government site or any other site in performance of this contract, the contractor shall have this travel approved by, and coordinated with, the FEDSIM COR. Notification shall include, at a minimum, the number of persons in the party, traveler name, destination, duration of stay, purpose, and estimated cost. Prior to any long-distance travel, the contractor shall prepare a Travel Authorization Request for Government review and approval. Long-distance travel will be reimbursed for cost of travel comparable with the FTR.

Requests for travel approval shall:

a. Be prepared in a legible manner.
b. Include a description of the travel proposed including a statement as to purpose.
c. Be summarized by traveler.

d. Identify the TO number.
e. Identify the CLIN and IA associated with the travel.
f. Be submitted in advance of the travel with sufficient time to permit review and approval.

The contractor shall use only the minimum number of travelers and rental cars needed to accomplish the task(s). Travel shall be scheduled during normal duty hours whenever possible.

7.8 INTELLECTUAL PROPERTY RIGHTS

The existence of any patent, patent application or other intellectual property right that encumbers any deliverable must be disclosed in writing on the cover letter that accompanies the delivery. If no such disclosures are provided, the data rights provisions in FAR 52.227-14 apply.

7.9 ENERGY STAR AND FEMP-DESIGNATED ENERGY EFFICIENT PRODUCTS

The Energy Policy Act (EPAct) of 2005 requires Federal agencies to purchase Energy Star and Federal Energy Management Program (FEMP)-designated energy efficient products. The contractor shall provide products that earn the Energy Star and meet the Energy Star specifications for energy efficiency. The contractor is encouraged to visit energystar.gov for complete product specifications and updated lists of qualifying products.

Additionally, the Energy Independence and Security Act (EISA) of 2007 requires Federal agencies to purchase products that use low wattage during standby mode. The contractor shall use low wattage products wherever possible or as required under this TO.

The Electronic Product Environmental Assessment Tool (EPEAT) was created to define what it means for electronic products to be “environmentally preferable. The EPEAT standard has three tiers: Bronze, Silver, and Gold. Bronze means the product meets the mandatory criteria, Silver means the product meets the mandatory criteria plus 50% of the optional criteria, and Gold means the products meets the mandatory criteria plus 75% of the optional criteria. GSA’s policy is to purchase EPEAT-Silver products and encourages its contractors to do the same. The contractor shall ensure that for those products covered by an EPEAT standard, 95% of the products are EPEAT-registered.

7.10 HUBZONE REPRESENTATION

The contractor is required to complete and sign a HUBZone Small Business Concern Representation Statement in which the contractor represents that it is a HUBZone small business concern listed on the List of Qualified HUBZone Small Business Concerns maintained by the Small Business Administration (SBA) at http://dsbs.sba.gov/dsbs/search/dsp_searchhubzone.cfm, and no material changes in ownership and control, principal office, or HUBZone employee percentage have occurred since it was certified in accordance with 13 CFR part 126. CTA members are also each required to submit a representation statement.

The purpose of the representation statement is to verify that the contractor is a HUBZone small business concern at the time of its initial offer. The representation will be re-verified by the CO at the time of contract award, therefore to aid in checking the SBA List of Qualified HUBZone Small Business Concerns, the contractor must provide with its representation statement its Cage

Code, DUNS Number, and if applicable, its 8(a) Case Number. This requirement also applies to any CTA members.

8.1 52.252-2 CLAUSES INCORPORATED BY REFERENCE (FEB 1998)

This TO incorporates one or more clauses by reference with the same force and effect as if they were given in full text. Upon request the CO will make their full text available. Also, the full text of a provision may be accessed electronically at:

FAR website: https://www.acquisition.gov/far/

Clause No	Clause Title	Date
52.204-2	Security Requirements	(Aug 1996)
52.203-5	Covenant Against Contingent Fees	(Apr 1984)
52.203-6	Restrictions on Subcontractors Sales to the Government	(Sept 2006)
52.203-7	Anti-Kickback Procedures	(Oct 2010)
52.203-8	Cancellation, Recession, and Recovery of Recovery of Funds for Illegal or Improper Activity	(Jan 1997)
52.203-10	Price of Fee Adjustment For Illegal or Improper Activity	(Jan 1997)
52.203-12	Limitation on Payments to Influence Certain Federal Transactions	(Oct 2010)
52.203-13	Contractor Code of Business Ethics and Conduct	(Apr 2010)
52.203-14	Display of Hotline Posters: (3) link will be provided at time of award.	(Dec 2007)
52.204-2	Security Requirements	(Aug 1996)
52.204-7	Central Contractor Registration	(Feb 2012)
52.204-10	Reporting Executive Compensation and First-Tier Subcontract Awards	(Aug 2012)
52.215-2	Audit and Records – Negotiation	(Oct 2010)
52.215-10	Price Reduction for Defective Certified Cost or Pricing Data	(Aug 2011)
52.215-11	Price Reduction for Defective Certified Cost or Pricing Data—Modifications	(Aug 2011)
52.215-12	Subcontractor Certified Cost or Pricing Data	(Oct 2010)
52.215-13	Subcontractor Certified Cost or Pricing Data—Modifications	(Oct 2010)
52.215-15	Pension Adjustments and Asset Reversions	(Oct 2010)
52.217-8	Option to Extend Services Fill-In Date: 10 days	(Nov 1999)
52.217-9	Option to Extend the Term of the Contract Fill-In Date:15 days Fill-In Date:30 days Fill-In Date:5 years	(Mar 2000)
52.222-3	Convict Labor	(Jun 2003)
52.223-5	Pollution Prevention and Right-to-Know Information (Alternate II)	(May 2011)
52.223-6	Drug-Free Workplace	(May 2001)
52.223-10	Waste Reduction Program	(May 2011)
52.227-14	Rights in Data – General Alternates II and III	(Dec 2007)

Clause No	Clause Title	Date
52.227-15	Representation of Limited Rights Data and Restricted Computer Software	(Dec 2007)
52.227-16	Additional Data Requirements	(June 1987)
52.232-22	Limitation of Funds	(Apr 1984)
52.232-23	Assignment of Claims	(Jan 1986)
52.232-23	Assignment of Claims (Alternate I)	(Apr 1984)
52.237-10	Identification of Uncompensated Overtime	(Oct 1997)
52.243-3	Changes- Time and Materials or Labor Hours	(Sep 2000)
52.244-5	Competition in Subcontracting	(Dec 1996)
52.244-6	Subcontracts for Commercial Items	(Dec 2010)
52.245-1	Government Property	(Apr 2012)
52.245-9	Use and Charges	(Apr 2012)
52.246-6	Inspection- Time and Material and Labor Hour	(May 2001)
52.246-23	Limitation Of Liability	(Feb 1997)
52.246-25	Limitation of Liability – Services	(Feb 1997)
52.247-14	Contractor Responsibility for Receipt of Shipment	(Apr 1984)
52.249-14	Excusable Delays	(Apr 1984)
52.251-1	Government Supply Sources	(Aug 2012)
52.253-1	Computer Generated Forms	(Jan 1991)

8.2 GENERAL SERVICES ADMINISTRATION ACQUISITION MANUAL (GSAM) CLAUSES INCORPORATED BY REFERENCE

The full text of a provision may be accessed electronically at:

GSAM website: https://www.acquisition.gov/gsam/gsam.html

Clause No	Clause Title	Date
552.232.25	Prompt Payment	(Nov 2009)
552.239-71	Security Requirements for Unclassified Information Technology Resources	(Jan 2012)

9.1 LIST OF ATTACHMENTS

Attachment	Title
A	COR Appointment Letter (provided as separate attachment)
B	Monthly Status Report
C	Travel Authorization Template (provided as separate attachment)
D	Corporate Non-Disclosure Agreement (provided as separate attachment)
E	Corporate Experience Template
F	Government-Furnished Property (provided as separate attachment)
G	Problem Notification Report
H	Acronym List (provided as separate attachment)
I	Deliverable Acceptance-Rejection Report
J	Key Personnel Qualification Matrix (To be removed at time of award)
K	Project Staffing Plan Template (To be removed at time of award) (provided as separate attachment)
L	Question and Answer Template
M	GSA Procedural Guide: CIO IT Security-06-30 (provided as separate attachment)
N	GSA Procedural Guide: CIO IT Security-09-44 (provided as separate attachment)
O	PCI DSS Requirements and Security Assessment Procedures (provided as separate attachment)
P	GSA Procedural Guide: CIO IT Security-11-51 (provided as separate attachment)
Q	GSA IT Security Policy (GSA Order P.2100.1I) (provided as separate attachment)
R	GSA Procedural Guide: CIO IT Security-12-66 (provided as separate attachment)
S	GSA Procedural Guide: CIO IT Security-01-02 (provided as separate attachment)
T	GSA Order CPO 1871.1 “GSA Privacy Act Program” (provided as separate attachment)
U	GSA Procedural Guide: CIO IT Security-06-29 (provided as separate attachment)

ATTACHMENT A

COR Letter of Appointment

(provided as separate attachment)

ATTACHMENT B

MONTHLY STATUS REPORT FOR (MONTH)

Contractor Name
Task Order Number
Prepared by:
Reporting Period:
Page 1 of __

Monthly Status Report

Work Planned for the Month

Work Completed During the Month

Work Not Completed During the Month

Work Planned for Next Month

Contract Meetings
Indicate the meeting date, meeting subject, persons in attendance and duration of the meeting.

Deliverable Status

Issues/Questions/Recommendations

Risks
Indicate potential risks, their probability, impact, and proposed mitigation strategy.

OCI Compliance Statement Attachment

ATTACHMENT C

Travel Authorization Template

(provided as separate attachment)

ATTACHMENT D

Corporate Non-Disclosure Agreement Template

(provided as separate attachment)

ATTACHMENT E

Corporate Experience Template

CORPORATE EXPERIENCE EXAMPLE (insert #) Program/Project Title:	Task Order Number:
Dollar value of the cited project:	Period of Performance:
Performing Business Unit:	
Client Agency:	Client Location:
Client POC #1 to contact (name, phone number and email):	Client POC #2 to contact (name, phone number and email):

a. Description of the work performed.
b. Types of Deliverables Required.

ATTACHMENT F

Government Furnished Property List

(provided as separate attachment)

ATTACHMENT G

Sample Problem Notification Report

PROBLEM NOTIFICATION REPORT

TASK ORDER NUMBER: _____ DATE: _____

1. Nature and sources of problem:

2. COTR was verbally notified on: (date) _____

3. Is action required by the Government? Yes_____ No_____

4. If YES, describe Government action required and date required:

5. Will problem impact delivery schedule? Yes_____ No_____

6. If YES, identify what deliverables will be affected and extent of delay:

7. Can required delivery be brought back on schedule? Yes_____ No_____

8. Describe corrective action needed to resolve problems:

9. When will corrective action be completed?

10. Are increased costs anticipated? Yes_____ No_____

11. Identify amount of increased costs anticipated, their nature, and define Government responsibility for problems and costs:

ATTACHMENT H

RFQ Acronym List

(provided as separate attachment)

ATTACHMENT I

Sample Deliverable Acceptance/Rejection Report

DELIVERABLE ACCEPTANCE/REJECTION FORM

Dear (insert name of COTR)

Please review the deliverable identified below, sign and date, and provide any comments either in the space provided or on an attached form. Comments are due by **XX/XX/20XX**.

DELIVERABLE NAME:
AGENCY NAME:
PROJECT NAME:
FEDSIM TASK ORDER/CONTRACT NUMBER:
FEDSIM PROJECT NUMBER:
DELIVERABLE DUE DATE:

I have reviewed the aforementioned document and have:
☐ Accepted it without comments
☐ Accepted it with comments
☐ Rejected it with comments

COMMENTS:

_____ _____
(name) (date)
(title)

ATTACHMENT J

Key Personnel Qualification Matrix (To be removed at time of award)

EXAMPLE - The following is an example of how the matrix shall map to Section H of the task order. The example detailed below describes a case in which the task order requires a Senior Network Engineer:

7.X.X.X Senior Network Engineer

It is desirable that the Senior Network Engineer have significant experience managing the design, development, implementation, testing, and maintenance of large (over 100 servers, 1000 workstations, and 10 locations) local and wide area networks in a secure Federal Government environment. The Senior Network Expert should have IRM experience managing an integrated network with a diversity of users. The individual should be functionally proficient in the operations and maintenance of local, metropolitan, and wide area networks using automated network management tools, responding to both client and user requests for applications assistance and network modifications and enhancements. The Senior Network Engineer should have experience supervising at least thirty network support staff of various job categories and skills. The Senior Network Engineer should have broad-based skills and experience managing the migration of separate networks into single WAN, performing routine system maintenance and troubleshooting, managing the installation of software upgrades, maintaining network performance, and recommending enhancements.

The offeror for this example is proposing John Smith as a Senior IT Analyst. The Key Qualification Matrix would be formatted as follows:

KEY PERSONNEL QUALIFICATIONS MATRIX

Proposed Personnel Name: John Smith
Proposed meets the TO requirements (per 7.X.X.) for: Senior Network Engineer
Proposed meets the requirements of the Basic Contract for Labor Category: Senior IT Analyst
Proposed meets the TO Clearance Level requirements: Not a requirement for this position
Proposed person is available to begin work on the start date designated in Section 6.

Requirements	**Years of Experience**	**Description of qualifications and experience**
Task Order Request Section 7.9.8.2		
Experience managing the design, development, implementation, testing, and maintenance of large (over 100 servers, 1000 workstations, and 10 locations) local and wide area networks in a secure Federal Government environment		
IRM experience managing an integrated network with a diversity of users		
Functionally proficient in the operations and maintenance of local, metropolitan, and wide area networks using automated network management tools, responding to both client and user requests for applications assistance and network modifications and enhancements		
Experience supervising at least thirty network support staff of various job categories and skills		
Broad-based skills and experience managing the migration of separate networks into a single WAN, performing routine system maintenance and troubleshooting, managing the installation of software upgrades, maintaining network performance, and recommending enhancements		

Note: Multiple pages for qualifications are acceptable.

See page limitations in section **11.8.2 KEY PERSONNEL QUALIFICATION MATRIX.**

END OF EXAMPLE

ATTACHMENT K

Sample Project Staffing Plan Template

(provided as separate attachment)

ATTACHMENT L

Question and Answer Template

Company Name:
Solicitation Number: GSC-QF0B-14-32845

Note to offerors: Please provide the specific paragraph reference using the Section/sub-Section numbers in the solicitation.

PARAGRAPH #	PARAGRAPH TITLE	QUESTION	GOVERNMENT RESPONSE

ATTACHMENT M

GSA Procedural Guide: CIO IT Security-06-30

(provided as separate attachment)

ATTACHMENT N

DRAFT GSA Procedural Guide: CIO IT Security-09-44

(provided as separate attachment)

ATTACHMENT O

PCI DSS Requirements and Security Assessment Procedures

(provided as separate attachment)

ATTACHMENT P

GSA Procedural Guide: CIO IT Security-11-51

(provided as separate attachment)

ATTACHMENT Q

GSA IT Security Policy (GSA Order P.2100.1I)

(provided as separate attachment)

ATTACHMENT R

GSA IT Security Policy 12-66

(provided as separate attachment)

ATTACHMENT S

GSA IT Security Policy 01-02

(provided as separate attachment)

ATTACHMENT T

GSA Privacy Act Program

(provided as separate attachment)

ATTACHMENT U

GSA IT Security Policy 06-29

(provided as separate attachment)

11.1 52.252-1 SOLICITATION PROVISIONS INCORPORATED BY REFERENCE (FEB 1998)

This solicitation incorporates one or more solicitation provisions by reference, with the same force and effect as if they were given in full text. Upon request, the CO will make their full text available. The offeror is cautioned that the listed provisions may include blocks that must be completed by the offeror and submitted with its quotation or offer. In lieu of submitting the full text of those provisions, the offeror may identify the provision by paragraph identifier and provide the appropriate information with its quotation of offer. The solicitation provisions and/or contract clauses are available in either HTML or PDF format at:

http://www.acquisition.gov/far.

Clause No	Clause Title	Date
52.215-1	Instructions to Offerors-Competitive Acquisition	(Jan 2004)
52.215-20	Requirements for Cost or Pricing Data or Information Other Than Cost or Pricing Data – Alternate IV	(Oct 2010)
52.232-38	Submission of Electronic Funds Transfer Information with Offer	(May 1999)

11.2 GENERAL INSTRUCTIONS

a. Offerors shall furnish the information required by this solicitation. A Standard Form (SF) 18, "Request for Quotation," completed and signed by the offeror, Block 14, constitutes the offeror's acceptance of the terms and conditions of the proposed TO. Therefore, the SF 18 must be executed by a representative of the offeror authorized to commit the offeror to contractual obligations.

b. Offerors are expected to examine this entire solicitation document including the Contract. Failure to do so will be at the offeror's own risk.

c. The Government may make award based on initial offers received, without discussion of such offers. Quotes shall set forth full, accurate, and complete information as required by this solicitation package (including Attachments). The penalty for making false statements in quotes is prescribed in 18 U.S.C. 1001.

d. Offerors submitting restrictive data will mark it as follows in accordance with the FAR 52.215-1, Instructions to Offerors - Competitive Acquisition, which is incorporated by reference. Clause 52.215-1 states: "Offerors who include in their proposals data they do not want disclosed to the public for any purpose or used by the Government except for evaluation purposes, shall –

Mark the title page with the following legend:

"This quote includes data that shall not be disclosed outside the Government and shall not be duplicated, used or disclosed--in whole or in part--for any purpose other than to evaluate this quote or quotation. If, however, a TO is awarded to this offeror as a result of--or in connection with--the submission of this data, and the Government incorporates the quote as part of the award, the Government shall have the right to duplicate, use, or

disclose the data. Also, this restriction does not limit the Government's right to use information contained in this data if it is obtained from another source without restriction. The data subject to the restriction is contained in sheets (insert numbers or other identification of sheets)"; and

Mark each sheet of data it wishes to restrict with the following legend:

"Use or disclosure of data contained on this sheet is subject to the restriction on the title page of this quote."

e. The Government assumes no liability for disclosure or use of unmarked data and may use or disclose the data for any purpose. Unless restricted, information submitted in response to this request may become subject to disclosure to the public pursuant to the provisions of the Freedom of Information Act (5 U.S.C. 551).

f. The authorized negotiator or the signatory of the SF 18 will be notified of the date and time of the oral technical quote presentation. Offerors shall provide the name of the individual, the position title, telephone number, fax number, and electronic mail address of that individual.

11.3 SUBMISSION OF QUESTIONS

Offerors are requested to submit their questions grouped by solicitation Section and make reference to the particular Section/Subsection number. Questions must be received before the date specified for receipt of questions using the format in Section 9, List of Attachments, Attachment L. **Questions or requests for extension submitted after the cut-off date will not be considered.**

Any information given to a prospective offeror concerning this solicitation will be furnished promptly to other prospective offerors as an amendment to the solicitation.

11.4 AVAILABILITY OF EQUIPMENT AND SOFTWARE

All commercial hardware and software proposed in response to this solicitation document shall have been formally announced for general release on or before the closing date of the solicitation. Failure to have equipment or software announced prior to submission of quote may render the offeror’s quote unacceptable.

11.5 GENERAL INFORMATION

The estimated total level of effort of T&M CLINs X001 and X002 of this TO is between **351,775 and 390,861 hours.**

11.6 SUBMISSION OF OFFERS

Each offer shall be in three parts.

The offeror shall submit all on the due date indicated on SF 18.

11.6.1 PROPOSAL PART I

Part I is the written Price quote and shall contain the following:

a. Request for Quotation (SF 18) (TAB A)

b. Supplies or Services and Prices (TAB B)
c. Price Supporting Documentation (TAB C)
d. Subcontractor Supporting Documentation (TAB D)
e. Cost/Pricing Assumptions (TAB E)
f. Organizational Conflict of Interest Statement (TAB F)
g. Contractor Registration (TAB G)
h. Price Explanation (TAB H)
i. HUBZone Representation (TAB I)

11.6.2 PROPOSAL PART II

Part II is the written Technical quote and shall contain the following:

a. Project Staffing Plan Table (TAB AA) (no limit)
b. Key Personnel Qualification Matrix, including Letters of Commitment (TAB BB) (limited to six pages for each Key Person, including additional Key Personnel proposed by the offeror; the Letter of Commitment counts as one of those six pages)
c. Corporate Experience (TAB CC) (limited to five pages per experience reference)
d. Section 508 Compliance Statement (TAB DD)
e. Technical Assumptions (if any) (TAB EE)

Pass/Fail criteria are part of this submission. See Section 12.4.

11.6.3 PROPOSAL PART III

Part III is the separately bound slides for the oral technical quote presentation and shall contain the following:

a. Key Personnel and Project Staffing

b. Technical and Management Approach

~~c. Corporate Experience~~

The CO will schedule the oral technical quote presentation after all offers are received. The oral technical quote presentation shall contain the information shown in the paragraphs in section 11.10.

11.7 SUBMISSION OF THE WRITTEN PRICE QUOTE (PART I)

Written Price Quotes shall be submitted as an original, one paper copy, and two electronic copies (CD or DVD). The offeror shall submit all proposed costs using Microsoft Excel software utilizing the formats without cells locked and include all formulas. The quote shall contain the following tabs:

a. Request for Quotation (SF 18) (Tab A). When completed and signed by the offeror, constitutes the offeror's acceptance of the terms and conditions of the proposed TO. Therefore, the form must be executed by representatives of the offeror authorized to commit the offeror to contractual obligations. Offerors shall sign the SF 18 in Block #14.

b. Supplies or Services and Prices/Costs (Tab B). The offeror shall indicate the price to be charged for each item in Section 1 - Supplies or Services and Price/Costs rounded to the nearest whole dollar.

c. Price Supporting Documentation (Tab C). The information requested in the quote is required to enable the Government to perform a cost or price analysis. The offeror shall prepare one summary schedule (Section 1 – Supplies or Services and Prices/Costs) which provides the total NTE or FFP amount for each CLIN and the total NTE or FFP price offered. Along with the summary schedule, the offeror is required to provide full back-up documentation for each CLIN and proposed Task Area. The back-up documentation shall detail the labor categories to be used, labor hours proposed by category, schedule labor rate, and proposed task order labor rate. The offeror shall identify the discounts offered by the offeror and/or the offeror's CTA member(s).

d. Subcontractor Supporting Documentation (Tab D). Both GSA Schedule Contractor Team Arrangements (CTA) and subcontracting are permissible under this RFQ. If a CTA arrangement is proposed, the offeror must submit the CTA under this tab. Additionally, each CTA member shall provide a copy of their applicable GSA Schedule Price List to substantiate the rates offered. If subcontracting is proposed, all labor and materials proposed must be contained within the prime contractor's GSA Schedule Contract. Furthermore, the prime contractor shall disclose to the Government's CO a copy of the subcontract pricing, terms and conditions, or teaming agreement. The Government will evaluate the acceptability of any subcontracting or teaming arrangement as part of its evaluation of price. Failure to provide complete supporting documentation may result in no further consideration of the offeror's quote. Cost/Pricing Assumptions (Tab E). Offerors must submit, under a separate tab, all (if any) assumptions upon which the Cost/Price Quote is based.

e. Organizational Conflict of Interest Statement (Tab F). The offeror shall complete and sign an OCI Statement in which the offeror (and any subcontractors, consultants, or CTA members) disclose information concerning actual or potential OCI affecting the offeror's proposal or any work related to this RFQ. The statement should be accompanied by the offeror's plan for mitigation, avoidance, or neutralization, if appropriate.

f. Contract Registration (Tab G). The offeror shall submit a statement that the contract vehicle under which this quote is being submitted has been registered in TOS (https://portal.fas.gsa.gov) and that all information in TOS is up-to -date.

g. Price Explanation (Tab H). The offeror shall describe why the total level of effort of the TO is above or below the labor mix shown in Section 11.5. The offeror shall include an explanation that specifically draws the Government's attention to any unique technical aspects of the proposal the offeror would like the Government to consider as the justification for the deviation from the range.

h. HUBZone Representation (Tab I). The offeror shall complete and sign a HUBZone Small Business Concern Representation Statement representing the offeror's and all CTA members' status as a HUBZone small business concern.

Pursuant to Section 11.6, offerors shall not include any price data in the technical quote.

11.8 SUBMISSION OF THE WRITTEN TECHNICAL QUOTE, PART II

Each offeror shall submit all information described in the following paragraphs. The offeror shall provide an original, four paper copies, **and 3 electronic copies (CD or DVD)** containing all required Sections of this Part. Please note that that the written technical quote shall be separately bound from the oral technical presentation slides as stated in Section 11.10.

11.8.1 PROJECT STAFFING PLAN TABLE (TAB AA)

The offeror shall provide a Project Staffing Plan Table in accordance with the Project Staffing Plan Table Template contained in Section 9 - List of Attachments, Attachment K. The submission shall contain all individuals that will be working on this effort. All Key Personnel proposed shall be available to begin work immediately on the Project Start Date indicated in Section 5 of this solicitation.

If the names of all non-Key Personnel are not known prior to offer submission, the offeror may indicate "to be determined" in the Project Staffing Plan Table. The names of non-Key Personnel are the only identifiers that may remain unspecified in the Project Staffing Plan Table. The names of all non-Key Personnel that can be provided shall be provided.

11.8.2 KEY PERSONNEL QUALIFICATION MATRIX (TAB BB)

The offeror shall submit a Key Personnel Qualification Matrix for each Key Person proposed relating the specialized experience identified in Section 7.1 of this TO and the qualifications of the person or persons being proposed for that position. For those additional Key Personnel proposed, the offeror shall identify the specialized experience and the corresponding qualifications for this experience. Each Key Personnel Qualification Matrix shall be limited to six pages, including the Letter of Commitment.

The offeror shall represent the following:

a. All Key Personnel meet the requirements of the offeror's IT Schedule 70 Contract.
b. All Key Personnel meet the requirements of the TO including security requirements in Section 7.4.
c. All Key Personnel named are available to begin work on the Project Start Date designated in Section 5 - Deliverables or Performance.
d. Letter of Commitment, signed by each proposed Key Person at the proposal submission due date. Currently employed key personnel are not exempt from this requirement.

11.8.3 CORPORATE EXPERIENCE REFERENCES (TAB CC)

The offeror shall provide recent (started within the past five years) Corporate Experiences for three projects similar in size, scope, and complexity to the requirements of this TO. One of these three corporate experiences shall be the offeror's direct Corporate Experience as the prime contractor. Two of the Corporate Experiences may be the offeror's direct Corporate Experience as the prime or subcontractor or the direct Corporate Experience of a proposed subcontractor performing as a prime contractor on that Corporate Experience project. Corporate Experience

where the offeror proposing to perform as the prime contractor on this TO served as the prime contractor for the proposed Corporate Experience will be treated more favorably.

These three projects must be similar in size, scope, **and** complexity to the requirements identified in Section 2. The Corporate Experience information must be submitted in the format provided in Section 9, List of Attachments - Attachment E. The offeror should ensure that all of the points of contact are aware that they may be contacted.

All three projects submitted shall be contracts or orders for the performance of actual technical requirements. Master contract vehicles, such as Blanket Purchase Agreements, Indefinite Delivery/Indefinite Quantity contracts, etc. do not satisfy the Corporate Experience requirement.

11.8.4 SECTION 508 COMPLIANCE STATEMENT (TAB DD)

The offeror's written quote shall include a statement indicating its capability to comply with Section 508 requirements throughout its performance of this TO in compliance with Section 7.5. Any quote that does not include a statement indicating the offeror's capability to comply with Section 508 requirements throughout its performance of this TO shall be eliminated from further consideration for award.

11.8.5 TECHNICAL ASSUMPTIONS (TAB EE)

Offerors shall identify and address assumptions affecting the technical proposal citing the component(s) of the proposal to which they pertain.

The Government reserves the right to reject any quote that includes any assumption that adversely impacts the Government's requirements.

11.9 DELIVERY INSTRUCTIONS

Offerors shall deliver written proposals and receive acceptance from:

Angela Holden
GSC-QF0B-14-32845
FEDSIM Project Number GS00658
GSA FAS AAS FEDSIM
1800 F Street NW
Suite 3100 (QF0B)
Washington, DC 20405

Quotes not received by 11:00 a.m. Eastern Time (ET) on the date stated in the cover letter will not be considered.

11.10 PART III – ORAL TECHNICAL QUOTE PRESENTATION

Each offeror shall make an oral technical quote presentation and participate in a question and answer (Q&A) session led by the CO and participated in by the Technical Evaluation Board (TEB) Members and other representatives of the Government. The offeror must be prepared to answer questions about the oral technical proposal presentation and the written technical proposal in the Q&A session. The oral technical quote presentation and Q&A session will be held at the unclassified level. The oral technical quote presentation will be used to assess the offeror's capability to satisfy the requirements set forth in the RFQ. The offeror's oral technical

quote presentation shall contain the information in Section 11 - Instructions, Conditions, and Notices to Offerors and Respondents.

The contents of all quotes will be delivered to FEDSIM at the same time. The oral technical proposal presentation, Part III, shall be separately bound from Parts I and II. **The offeror shall provide an original, four paper copies, and three electronic copies (CD or DVD) containing all required Sections of this Part.**

Oral technical proposal presentation slides presented that differ from slides delivered with the technical proposal will not be evaluated.

11.10.1 ORAL TECHNICAL QUOTE PRESENTATION CONSTRAINTS

The offeror shall identify the authors of the presentation by name and association with the offeror. Attendance at the presentation and the subsequent Q&A session shall be limited to the offeror's Key Personnel (all Key Personnel are highly encouraged to attend) and no more than three additional corporate representatives of the offeror. An offeror's "Key Personnel" includes only those persons who will be assigned to the TO as Key Personnel as described in Section 7 - Special Contract Requirements. The three additional people (e.g., CEO's, company presidents, or contract representatives) from the offeror may attend, but will not be allowed to participate in the presentation. Any of the three additional personnel may make a brief introduction which will not be evaluated, but will count towards the offeror's allotted time. For the remainder of the presentation, only Key Personnel shall present.

The offeror will be given 15 minutes for set up. After opening remarks by the Government, the offeror will be given up to 60 minutes to present. The presentation will be stopped precisely after 60 minutes.

Upon completion of the presentation, the Government will caucus to formulate any questions regarding the technical quote. The Government and offeror will then address any questions or clarifications posed by the CO or the TEB Chairman. The offeror may briefly caucus in the room to coordinate responses to specific requests for clarification. The CO and the TEB Chairman will be responsible for ensuring the schedule is met and that all offerors are given the same opportunity to present and answer questions. Offerors shall provide four appropriately bound hard copies of the presentation materials (including slides, transparencies).

11.10.2 ORAL TECHNICAL QUOTE PRESENTATION MEDIA

There is no limit to the number of slides that can be presented during the oral technical presentation, but only those slides actually presented during the oral presentation will be considered for evaluation. Offerors need to address points on each slide to be considered. Any slides over and above those presented during the oral presentation will be returned to the offeror and will not be evaluated as part of this source selection. No other media may be used. Presentation media is limited to computer-based graphics of the offeror's choice displayed using an appropriate projector. Unobtrusive company logos or names can be inserted in any or all slides. Slides should be sequentially numbered in the lower right corner. Transition effects shall not be used. The slides shall not contain any fonts smaller than a proportionally spaced font (such as Times New Roman) of at least 12 point.

Except for the screen provided in the conference room, the Government will provide no equipment. The offeror shall be responsible for any equipment necessary for the presentation.

11.10.3 ORAL TECHNICAL QUOTE PRESENTATION SCHEDULING

The CO will schedule the oral technical quote presentation with the authorized negotiator or the signatory of the SF 18. Time slots will be assigned randomly and may not be changed or traded. The Government reserves the right to reschedule any offeror's oral technical quote presentation at its sole discretion.

Oral Technical Quote Presentations will be given at facilities designated by the CO. The exact location, seating capacity, and any other relevant information will be provided when the presentations are scheduled.

11.10.4 RECORDING OF THE ORAL TECHNICAL QUOTE PRESENTATION

The offeror may **not** record or transmit any of the oral presentation process. All offeror's electronic devices shall be removed from the room while the Government is caucusing after the oral presentation.

11.10.5 ORAL TECHNICAL QUOTE PRESENTATION TOPICS

The Government does not expect the offeror to provide a thorough presentation of those items already submitted in writing in Part II. Instead, the offeror shall address this information under the topics provided. The oral technical quote presentation shall include the following topics, and be organized in the following order:

a. Topic 1: Key Personnel and Project Staffing Approach
b. Topic 2: Technical and Management Approach

11.10.5.1 KEY PERSONNEL AND PROJECT STAFFING (TOPIC 1)

During the oral presentation, the offeror shall describe the level of effort and skills it intends to utilize to support the requirements of the TO, including the estimated hours and labor mix, and the experience, skill, and qualifications of the personnel proposed (staffing plan will be completed in accordance with Section 11.8.2). The offeror should be sure to discuss Key Personnel and the currency and applicability of their experience as it relates to Section 7.1. The offeror's Key Personnel and Project Staffing approach shall describe:

a. The offeror's approach to hiring, retaining, and replacing the highly skilled technical staff who will perform the requirements of this Order.
b. The offeror's approach to staffing non-Key Personnel and the degree to which proposed non-Key Personnel hold appropriate accreditation or credentials as indicated by the offeror's staffing plan.
c. The rationale of the staffing approach and how it aligns with the offeror's proposed management approach.

11.10.5.2 TECHNICAL AND MANAGEMENT APPROACH (TOPIC 2)

The offeror shall identify and describe the methodology, techniques, and management approach to meet the requirements identified in each task of the RFQ. The offeror shall tailor its approach to achieve the best possible results in meeting GSA's requirements as identified in Section 2 –

Statement of Work. The Technical and Management Approach shall further describe the following:

a. The methodology and techniques to be used in fulfilling the requirements as outlined in the SOW.

b. The offeror's approach to migrating from the existing stove-piped security posture to a holistic, integrated GSA security posture.

c. The offeror's approach to adapting its processes to GSA's processes, and applying standards-based methodologies and resources in executing the requirements of this TO.

d. The offeror's approach to improving the GSA security posture and practices while executing the requirements of this order.

e. The offeror's approach to Tier 3 incident handling and incident response including experience with Forensic Investigations, malware analysis (re-engineering), and Advanced Persistent Threat. The offeror's discussion shall detail, using specific examples, how it plans to ensure response commensurate with the level of threat, and methodology for handling of forensic evidentiary data under this TO.

12.1 METHOD OF AWARD

The Government anticipates awarding a TO to the offeror whose quote is the most advantageous to the Government, price and other factors considered. Technical quotes will be evaluated based on the factors described in Section 12.4. All evaluation factors other than price, when combined, are significantly more important than price. Award will be made to the offeror whose quote is determined be the best value for the Government.

Quotes shall set forth full, accurate, and complete information as required by this solicitation package (including Attachments). The penalty for making false statements in quotes is prescribed in 18 U.S.C. 1001.

12.2 EXPLANATION FOR BASIS OF AWARD

This award will be made under FAR 8.4; formal debriefings will not be conducted. In accordance with 8.405-2(d), a brief explanation of the basis for the award decision shall be provided upon request. Requests for explanation must be received within 5 calendar days of award.

12.3 PRICE QUOTE EVALUATION

The offeror's written price quote will be evaluated by the Government. Prices that are excessively high or low (without sufficient justification) may be considered unrealistic and unreasonable and may receive no further consideration. A determination of price realism and reasonableness will also include a determination by the CO that proper discounts have been offered commensurate with maximum order thresholds for prime contractors and CTA members and in accordance with subcontractor arrangements. The Government reserves the right to reject any quote that includes any assumption that adversely impacts the Government's requirements.

The Government will evaluate each price quote for the realism and reasonableness of its pricing. The price realism determination will look at the labor mix and hours proposed. Price reasonableness will be determined by looking at whether the total price is reasonable, since labor and material rates set forth in GSA Schedule contracts are deemed fair and reasonable under FAR 8.404(d). Also, the Government will consider team discounts that are required to remain in effect for the period of performance of the TO.

12.3.1 ORGANIZATIONAL CONFLICT OF INTEREST

Tab F will be evaluated to assess whether or not an actual or potential OCI exists. If an actual or potential conflict of interest is identified that cannot be mitigated, avoided, or waived in accordance with FAR Part 9.5, that offeror will be ineligible for award.

12.3.2 PRICE ASSUMPTIONS

The Government reserves the right to reject any proposal that includes any price assumptions that may adversely impact satisfying the Government's requirements.

12.3.3 OVERTIME AND EXTENDED BILLING HOUR PRACTICES

The Government reserves the right to reject any proposal that includes overtime or extended hours billing practices that adversely impact or affect the Government's requirements.

12.4 TECHNICAL EVALUATION FACTORS

The Government will evaluate technical quotes (Section 11 - Instructions, Conditions, and Notices to Offerors or Respondents, Part II and Part III) based on the following factors:

Factor 1: Key Personnel and Project Staffing as shown on the written Project Staffing Plan Table/Key Personnel qualifications (Section 7.1, 11.8.1, 11.8.2, and 11.10.5.1)

Factor 2: Technical and Management Approach (Section 11.8) as well as the information presented under the Technical and Management approach factor (Section 11.10.5.2) as part of the oral technical presentation.

Factor 3: Corporate Experience (Section 11.8.3). ~~as well as the information presented under the corporate experience factor (Section 11.10.5.3) as part of the oral technical presentation.~~

The technical evaluation factors are listed in descending order of importance. All three technical factors combined are significantly more important than price. The Government will combine the results of the written and oral submissions to arrive at a rating for the technical evaluation factors as a whole. The receipt of an evaluation rating of Not Acceptable in any single Factor will result in the overall quote being determined Not Acceptable and therefore ineligible for award. **A failure on any single Pass/Fail criteria will make the quote ineligible for award, with no further evaluation of the technical and pricing quote accomplished by the Government.**

Pass/Fail Elements:
The following

a. The Government will reject any quote that does not provide a name for each Key Person proposed at the quote submission due date. A quote that states, "To Be Determined" or TBD for a proposed Key Person, or omits a Key Person, will be rejected by the Government (Section 11.8.2). The Government will reject any quote that does not provide a Letter of Commitment, signed by each proposed Key Person, at the quote submission due date. Key Personnel currently employed by the offeror or a member of the offeror's team or corporate group are not exempt from this requirement. All requirements for Key Personnel apply to any additional Key Personnel proposed by the offeror (Section 11.8.2).
b. The offeror and all CTA members (if any) do not each possess the required Schedule IT 70 SIN 132-51).
c. The Government will reject any proposal that does not include a HUBZone Small Business Concern Representation Statement stating that the offeror and all CTA members are HUBZone concerns **(**Section 7.11).
d. The Government will reject any quote that does not provide a Section 508 Compliance Statement (Section 11.6.4).

12.4.1 FACTOR 1: KEY PERSONNEL AND PROJECT STAFFING

The project staffing plan will be evaluated to assess the degree to which it provides an appropriate level of effort and skills to support the requirements of the TO, including the estimated hours and labor mix, and the experience, skill, and qualifications of the personnel proposed (staffing plan will be completed in accordance with Section 11.8.1). The Key Personnel matrix will be evaluated to assess the appropriateness and completeness of the

experience, skill, and qualifications of the proposed Key Personnel identified in Section 7.1. Key Personnel will also be evaluated to assess the currency and applicability of experience as it relates to Section 7.1. The following are not subfactors and will not be separately evaluated. The offeror's Key Personnel and Project Staffing approach will be evaluated based on the degree to which it demonstrates:

a. A clear, relevant, comprehensive, and detailed approach to hire, retain, and replace the highly skilled Key Personnel who will perform the requirements of this TO;

b. A clear, relevant, detailed, and comprehensive approach to staffing for all non-Key Personnel and the degree to which proposed non-Key Personnel hold appropriate accreditation or credentials as indicated by the offeror's staffing plan.

c. A clear, relevant, detailed, and comprehensive approach that demonstrates the rationale of the staffing approach and congruence with the offeror's proposed management approach.

12.4.2 FACTOR 2: TECHNICAL AND MANAGEMENTAPPROACH

The Government will evaluate the degree to which the offeror's Technical and Management Approach reflects an effective, efficient, feasible approach to accomplishing the tasks and deliverables of this TO. Specifically, the Government will evaluate the degree to which the offeror's Technical Approach complies with the requirements and deliverables of the RFQ and Section 11.10.5.1. The Government will also evaluate the project management strategy including indicators showing how the project will be implemented and the offeror's ability to manage resources. The following are not subfactors and will not be separately evaluated. The offeror's management approach will be evaluated based on the degree to which it demonstrates it has a clear, relevant, detailed, and comprehensive approach:

a. To fulfilling each of the requirements as outlined in the SOW.

b. To migrating from the existing stove-piped security posture to a holistic, integrated GSA security posture.

c. To adapting the offeror's processes to GSA's processes, and applying a standards-based methodologies and resources in executing the requirements of this TO.

d. To improving GSA's security posture and practices while executing the requirements of this TO.

e. To Tier 3 incident handling and incident response including experience with Forensic Investigations, malware analysis (re-engineering), and Advanced Persistent Threat. The offeror's discussion shall detail, using specific examples, how it plans to ensure response commensurate with the level of threat, and methodology for handling of forensic evidentiary data under this TO.

12.4.3 FACTOR 3: CORPORATE EXPERIENCE

The Corporate Experience factor will be evaluated based on the degree to which the offeror's Corporate Experience reflects/identifies experience on projects that are similar in size, scope, and

complexity to the requirements contained Section 2 - Description/ Specification/Statement of Work in the RFQ.

12.5 TECHNICAL ASSUMPTIONS

Offeror assumptions will be reviewed in the context of the technical factor to which they apply. The Government reserves the right to reject any quote that includes any assumption that may adversely impact satisfying the Government's requirements.